ESET ENDPOINT SECURITY für ANDROID

Benutzerhandbuch

(für Produktversion 2.0 und höher)

Klicken Sie hier, um die neueste Version dieses Dokuments herunterzuladen.

ESET **ENDPOINT SECURITY**

© ESET, spol. s r.o.
ESET Endpoint Security wurde entwickelt von ESET, spol. s r.o.
Nähere Informationen finden Sie unter www.eset.de.
Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Einwilligung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnehmen, Scannen oder auf andere Art.
ESET, spol. s r.o. behält sich das Recht vor, ohne vorherige Ankündigung an jedem der hier beschriebenen Software-Produkte Änderungen vorzunehmen.

Support: www.eset.com/support

Versionsstand 28. 8. 2015

Inhalt

1. Einführung 5
1.1 Neuerungen in Version 2 5
1.2 Mindestsystemanforderungen 9
2. Verbindungen von Benutzern mit ESET Remote Administrator 10
2.1 ESET Remote Administrator-Server 11
2.2 Web-Konsole 11
2.3 Proxy 12
2.4 Agent 12
2.5 RD Sensor 12
3. Remote-Installation 13
4. Lokale Installation auf dem Gerät 13
4.1 Download von der ESET-Website 14
4.2 Download aus Google Play 14
4.3 Startassistent 15
5. Deinstallation 16
6. Produktaktivierung 16
7. Virenschutz 17
7.1 Automatische Scans 18
7.2 Scan-Logs 19
7.3 Erweiterte Einstellungen 20
8. Anti-Theft 21
8.1 Administratorkontakte 22
8.1.1 Hinzufügen eines Administratorkontakts 23
8.2 Informationen der Bildschirmsperre 23
8.3 Vertrauenswürdige SIM-Karten 23
8.4 Remotebefehle 23
9. Anwendungskontrolle 24
9.1 Blockierregeln 25
9.1.1 Nach Anwendungsname blockieren 25
9.1.1.1 So blockieren Sie Anwendungen auf Grundlage des Anwendungsnamens 26
9.1.2 Blockieren nach Anwendungskategorie 26
9.1.2.1 Blockieren einer Anwendung auf Grundlage der Anwendungskategorie 26
9.1.3 Blockieren nach Anwendungsberechtigungen 27
9.1.3.1 So blockieren Sie Anwendungen auf Grundlage der Anwendungsberechtigungen 27
9.1.4 Unbekannte Quellen blockieren 27
9.2 Ausnahmen 28
9.2.1 Hinzufügen von Ausnahmen 28
9.3 Zugelassene Anwendungen 29
9.4 Berechtigungen 29
9.5 Verwendung 31
10. Gerätesicherheit 31

10.1 Policy für Bildschirmsperre 32
10.2 Policy für Geräteeinstellungen 33
11. Phishing-Schutz 34
12. SMS- und Anruffilter 35
12.1 Regeln 35
12.1.1 Hinzufügen einer neuen Regel 36
12.2 Verlauf 37
13. Einstellungen 37
13.1 Einstellungen importieren/exportieren 39
13.1.1 Einstellungen exportieren 40
13.1.2 Einstellungen importieren 40
13.1.3 Verlauf 40
13.2 Administratorpasswort 41
13.3 Remote administrator 42
13.4 Geräte-ID 42
14. Support 43

1. Einführung

Die neue Generation von ESET Endpoint Security für Android (EESA) ist auf die Verwendung mit ESET Remote Administrator (ERA) 6 ausgelegt, der neuen Verwaltungskonsole für die Remote-Verwaltung aller ESET-Sicherheitslösungen. ESET Endpoint Security für Android 2 ist nur mit ERA 6 und höher kompatibel.

für Android schützt die Mobilgeräte in Ihrem Unternehmen vor den neuesten Bedrohungen durch Schadcode und schützt außerdem die darauf enthaltenen Daten, falls das Gerät verloren geht oder gestohlen wird. Mit der Anwendung können Administratoren sicherstellen, dass die Geräte die Sicherheitsrichtlinien des Unternehmens erfüllen.

ESET Endpoint Security kann in kleineren oder mittelgroßen Unternehmen auch ohne die Remote-Verwaltung über ESET Remote Administrator bereitgestellt werden. IT-Techniker, Systemadministratoren und Endpoint-Benutzer können die eigene ESET Endpoint Security-Konfiguration mit Kollegen teilen. Mit dieser Funktion ist es nicht mehr nötig, nach der Installation von ESET Endpoint Security manuell das Produkt zu aktivieren und jedes Produktmodul einzeln einzurichten.

1.1 Neuerungen in Version 2

Anwendungskontrolle

Die Anwendungskontrolle bietet Administratoren die Möglichkeit, installierte Anwendungen zu überwachen, den Zugriff auf gesperrte Anwendungen zu unterbinden und das Gefahrenrisiko zu senken, indem Benutzer zur Deinstallation bestimmter Anwendungen aufgefordert werden. Weitere Informationen hierzu finden Sie im Abschnitt Anwendungskontrolle in diesem Handbuch.

Gerätesicherheit

Über den Bereich „Gerätesicherheit“ können Administratoren grundlegende Sicherheits-Policies auf mehreren Mobilgeräten anwenden. Dies bietet den Administratoren unter anderem folgende Möglichkeiten:

- Mindestsicherheitsstufe und Komplexität der Bildschirmsperrcodes festlegen
- Höchstanzahl nicht erfolgreicher Entsperrversuche festlegen
- Zeitintervall festlegen, nach dem die Benutzer ihren Bildschirmsperrcode ändern müssen
- Zeitgeber für die Bildschirmsperre definieren
- Kameraverwendung einschränken

Weitere Informationen hierzu finden Sie im Abschnitt Gerätesicherheit in diesem Handbuch.

Einstellungen importieren und exportieren

Um Einstellungen zwischen Mobilgeräten teilen zu können, wenn diese nicht mit ERA verwaltet werden, bietet ESET Endpoint Security 2 nun die Möglichkeit, Programmeinstellungen zu exportieren und importieren. Der Administrator kann die Geräteeinstellungen manuell in eine Datei exportieren und diese Datei (zum Beispiel per E-Mail) mit den Benutzern teilen. Die Datei kann auf einem beliebigen Gerät importiert werden, auf der die Clientanwendung ausgeführt wird. Wenn der Benutzer die Einstellungsdatei öffnet und akzeptiert, werden automatisch alle Einstellungen festgelegt und die Anwendung aktiviert (sofern die Lizenzinformationen enthalten waren). Alle Einstellungen sind mit dem Administratorpasswort geschützt.

Phishing-Schutz

Diese Funktion schützt die Benutzer vor dem Zugriff auf schädliche Websites, wenn sie einen unterstützten Webbrowser verwenden (standardmäßiger Android-Browser oder Chrome).

Die Anti-Phishing-Technologie schützt Benutzer vor Versuchen unseriöser, aber als seriös „getarnter“ Websites, an Passwörter, Bankdaten und andere sicherheitsrelevante Information zu gelangen. Wenn ein Gerät versucht, auf eine URL zuzugreifen, vergleicht der Anti-Phishing von ESET die URL mit einer ESET-Datenbank bekannter Phishing-Websites. Wenn eine Übereinstimmung erkannt wird, wird die Verbindung zur URL abgebrochen und eine Warnmeldung wird angezeigt.

Benachrichtigungszentrale

ESET Endpoint Security bietet Benutzern einen zentralen Benachrichtigungsbereich, wo alle Benachrichtigungen zu Anwendungsfunktionen angezeigt werden, die die Aufmerksamkeit des Benutzers erfordern. Die Benachrichtigungszentrale zeigt Informationen zu verschiedenen Ereignissen, Gründe für die Nichteinhaltung der Unternehmensrichtlinien und Vorschläge zum Erfüllen der Anforderungen. Die Benachrichtigungen sind nach Dringlichkeit sortiert. Benachrichtigungen mit höherer Priorität werden oben in der Liste angezeigt.

Neues Lizenzierungssystem

ESET Endpoint Security unterstützt ESET License Administrator, das neue Lizenzierungsmodell, das mit ESET Remote Administrator 6 eingeführt wurde.

Der neue Lizenzierungsrahmen vereinfacht die Bereitstellung und langfristige Nutzung von ESET-Sicherheitssoftware. Wenn ein Kunde eine Lizenzänderung anfordert, wird diese Änderung automatisch und auf transparente Weise in allen Produkten übernommen, die diese Lizenz verwenden. Die Kunden können daher Ihre E-Mail-Adresse und ein benutzerdefiniertes Passwort als Berechtigungsnachweis verwenden, anstelle des von ESET ausgegebenen Benutzernamens mit Passwort, wie es in älteren Produkten verwendet wird.

Die Einführung von Lizenzschlüsseln und automatischen Lizenzaktualisierungen (bei einer Verlängerung oder anderen Lizenzvorgängen) ermöglicht einen ununterbrochenen Schutz. Das ESET License Administrator-Portal und die Möglichkeit, Lizenzautorisierungsrechte nach E-Mail-Adresse (aus den Kontoinformationen des Kunden) zuzuweisen, vereinfacht die Lizenzverwaltung und -bereitstellung. Mit ESET License Administrator kann der Lizenzinhaber die Lizenzverwaltung an einen Verantwortlichen (auch einen Dritten) übertragen, behält jedoch dennoch die Kontrolle über die Lizenz.

Verwaltetes Upgrade eines Produkt auf einen neueren Build

Systemadministratoren, die ERA verwenden und ESET Endpoint Security für Android nicht sofort bei Verfügbarkeit auf eine neue Version aufrüsten möchten, können den Update-Mechanismus wie gewünscht steuern.

Einrichtungsassistenten

ESET Endpoint Security bietet Einrichtungsassistenten für ausgewählte Funktionen, um den Prozess nach der Installation möglichst unkompliziert zu halten.

Verbesserter Virenschutz

- Verkürzte Scan-Dauer des Echtzeit-Scans
- Integriertes ESET Live Grid
- 2 Scan-Stufen: Smart-Scan und Tiefen-Scan
- Verbesserungen des On-Demand-Scans: Scan im Hintergrund, Funktion zum Anhalten des Scans
- Geplante Scans: Der Administrator kann einen vollständigen Geräte-Scan planen.
- Scan während Ladevorgang: Ein Scan wird automatisch gestartet, sobald das Gerät im Ruhezustand (vollständig geladen und an ein Ladegerät angeschlossen) ist.
- Verbesserte Konfiguration der Updates der Signaturdatenbank: Der Administrator kann Zeiten für die regelmäßigen Updates festlegen und den zu verwendenden Update-Server festlegen (Release-Server, Testmodus-Server, lokaler Mirror).

Detaillierte Logs mit Scan-Ergebnissen werden an ERA gesendet. ESET Endpoint Security enthält Funktionen aus ESET Endpoint Security Version 1, wie die Erkennung potenziell unsicherer oder evtl. unerwünschter Anwendungen und USSD Control.

Verbesserter SMS- und Anruffilter

Der SMS- und Anruffilter, früher als „Spam-Schutz“ bezeichnet, schützt Benutzer vor unerwünschten Anrufen und SMS- und MMS-Nachrichten. Die Funktion bietet nun zwei Arten von Regeln: Administratorregeln und Benutzerregeln. Administratorregeln haben stets eine höhere Priorität.

Weitere Verbesserungen:

- Zeitbasiertes Blockieren: Der Benutzer oder der Administrator kann Anrufe und Nachrichten blockieren, die innerhalb bestimmter Zeiträume empfangen werden.
- Blockieren des letzten Anrufers oder Absenders, einer Telefonnummer, einer Kontaktgruppe oder verdeckter bzw. unbekannter Nummern durch einmaliges Tippen.

Verbesserte Anti-Theft-Funktion

Die Anti-Theft-Funktion trägt zum Schutz und Wiederfinden verloren gegangener oder gestohlener Geräte bei. Anti-Theft-Aktionen können über ERA oder über Remotebefehle ausgelöst werden.

In ESET Endpoint Security 2 können die gleichen Remotebefehle wie in Version 1 verwendet werden (Sperren, Daten löschen und Orten). Zusätzlich sind folgende neue Befehle verfügbar:

- **Entsperren** – entsperrt das gesperrte Gerät.
- **Erweitertes Zurücksetzen auf Werkseinstellungen** - Alle zugreifbaren Daten auf dem Gerät werden schnell gelöscht (Dateikopfdaten werden zerstört) und das Gerät wird auf die standardmäßigen Werkseinstellungen zurückgesetzt.
- **Sirene** - Das vermisste Gerät wird gesperrt und gibt einen sehr lauten Ton wider, selbst wenn es stumm geschaltet ist.

Um die Sicherheit der Remotebefehle zu erhöhen, empfängt der Administrator auf seinem Mobilgerät (unter der in der Administratorkontaktliste festgelegten Nummer) einen eindeutigen und zeitlich begrenzt gültigen SMS-Überprüfungscode, wenn er einen Remotebefehl ausführt. Dieser Überprüfungscode wird zur Überprüfung eines bestimmten Befehls verwendet.

Anti-Theft-Befehle in ERA

Die Anti-Theft-Befehle können nun auch in ERA ausgeführt werden. Mit der neuen Mobilgeräte-Verwaltungsfunktion können Administratoren mit nur wenigen Klicks Anti-Theft-Befehle senden. Die Tasks werden sofort über den Connector für Mobilgeräte, der nun Bestandteil der ERA-Infrastruktur ist, zur Ausführung gesendet.

Administratorkontakte

Dies ist die Liste der Administrator-Telefonnummern, die durch ein Administratorpasswort geschützt ist. Anti-Theft-Befehle können nur von vertrauenswürdigen Nummern aus gesendet werden.

Anzeigen einer Meldung aus ERA

Wenn Geräte remote verwaltet werden, kann der Administrator eine benutzerdefinierte Nachricht an ein bestimmtes Gerät oder eine Gerätegruppe senden. So können dringende Nachrichten schnell an die Benutzer der verwalteten Geräte übertragen werden. Die Meldung wird als Popup angezeigt, damit der Benutzer sie nicht übersehen kann.

Benutzerdefinierte Bildschirmsperren-Informationen

Der Administrator kann benutzerdefinierte Informationen (Firmenname, E-Mail-Adresse, Nachricht) festlegen, die angezeigt werden, wenn das Gerät gesperrt ist. Außerdem kann er festlegen, dass vordefinierte Administratorkontakte angerufen werden können.

Verbesserte Remote-Verwaltung mit ESET Remote Administrator **6**

Alle Anwendungseinstellungen können nun über eine Remote-Policy festgelegt werden, z. B. für den Virenschutz, SMS- und Anruffilter, Gerätesicherheitseinstellungen oder Einschränkungen der Anwendungskontrolle. So kann der Administrator die Sicherheitsrichtlinien des Unternehmens im gesamten Netzwerk erzwingen, auch auf Mobilgeräten.

ESET Endpoint Security für Android Version 2 bietet eine verbesserte Berichterstellung in der ERA-Web-Konsole. Dank ihr können Administratoren schnell problematische Geräte identifizieren und die Ursache des Problems ermitteln.

Die Verwaltung von Android-Geräten ist nun ein integrierter Bestandteil von ESET Remote Administrator 6. Nahezu alle Funktionen der ESET-Desktopprodukte wie ESET Endpoint Antivirus 6 und ESET Endpoint Security 6 können hier für Android-Geräte genutzt werden.

Lokale Verwaltung

ESET Endpoint Security für Android bietet Administratoren die Möglichkeit, Endgeräte lokal zu verwalten, wenn sie ESET Remote Administrator nicht verwenden möchten. Alle Anwendungseinstellungen werden mit dem Administratorpasswort geschützt, d. h. die Anwendung bleibt ständig unter vollständiger Kontrolle.

Verbesserte Verteilung und Installation des Produkts

Neben den üblichen Installationsmethoden (Herunterladen und Installieren eines Pakets von der ESET-Website oder Verteilen des Installationspakets per E-Mail) steht den Administratoren und Benutzer die Möglichkeit offen, die Anwendung über den Google Play Store herunterzuladen und zu installieren.

Verbesserte Produktaktivierung

Nach dem Herunterladen und Installieren stehen dem Administrator bzw. Benutzer mehrere Methoden zur Produktaktivierung zur Verfügung:

- Sie können die neuen Lizenzierungsoptionen nutzen und manuell den Lizenzschlüssel oder das Sicherheitsadministratorkonto eingeben.
- Sie können das Produkt durch Klicken auf den Link aktivieren, der vom Administrator per E-Mail gesendet wurde. Das Produkt konfiguriert automatisch die ERA-Verbindung. Die Lizenzinformationen werden von ERA zum Gerät übertragen.
- Der Administrator kann die ERA-Verbindungseinstellungen manuell eingeben.
- Beim Importieren der Datei mit den Anwendungseinstellungen (und enthaltenen Lizenzinformationen) wird die Anwendung dann aktiviert.

Verbesserte Identifizierung der Mobilgeräte in ERA

Während der Registrierung werden die Android-Geräte in die Positivliste aufgenommen und nur autorisierte Geräte können eine Verbindung zu ERA herstellen. Dies verbessert die Sicherheit und vereinfacht die Identifizierung einzelner Geräte: Jedes Mobilgerät kann über den Namen, eine Beschreibung und die IMEI identifiziert werden. Nur-WLAN-Geräte werden über die WLAN-MAC-Adresse identifiziert.

Neu gestaltete grafische Benutzeroberfläche

ESET Endpoint Security bietet ein besseres Benutzererlebnis, das mit dem der ESET-Lösungen für Geschäftskunden vergleichbar ist.

Benutzerfreundlichkeit

Die neue Benutzeroberfläche ermöglicht eine einfachere Bedienung und Navigation im Produkt. Die Struktur der grafischen Benutzeroberfläche entspricht der neuen Generation der ESET Endpoint-Lösungen und von ESET Remote Administrator.

1.2 Mindestsystemanforderungen

Für die Installation von ESET Endpoint Security muss das Android-Gerät folgende Mindestsystemanforderungen erfüllen:

- Betriebssystem: Android 4 (Ice Cream Sandwich) und höher
- Touchscreen-Auflösung: 480 x 800 px
- Prozessor: ARM mit ARMv7-Befehlssatz, x86 Intel Atom
- Freier Speicherplatz: 20 MB
- Internetverbindung

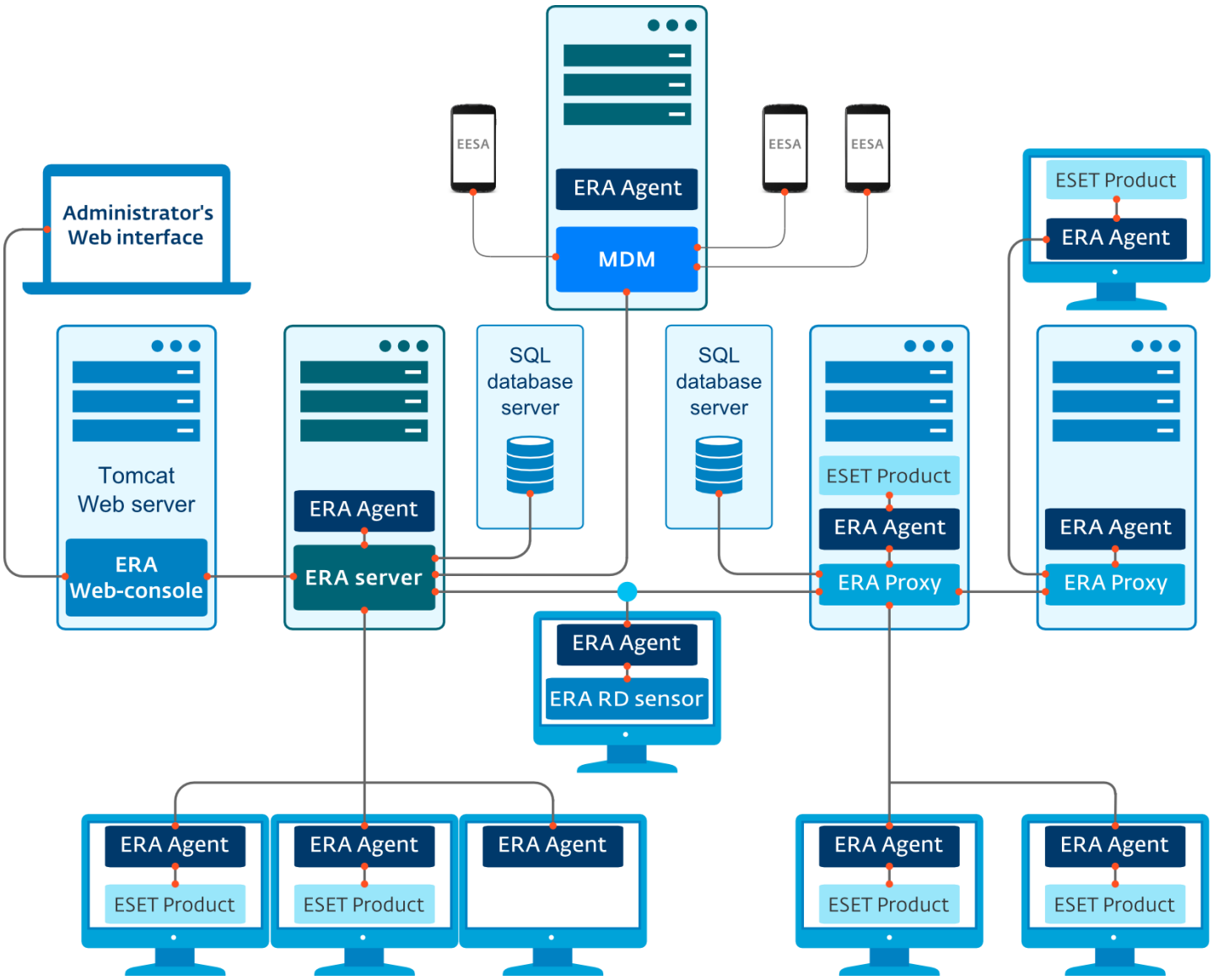
HINWEIS: Dual-SIM-Geräte und gerootete Geräte werden nicht unterstützt. Einige Funktionen (wie Anti-Theft und der SMS- und Anruffilter) sind auf Tablets ohne Unterstützung für Anruf-/Nachrichtenfunktionen nicht verfügbar.

2. Verbindungen von Benutzern mit ESET Remote Administrator

Mit ESET Remote Administrator (ERA) 6 können Sie ESET-Produkte in einer Netzwerkumgebung von einem zentralen Standort aus verwalten. Mit dem Task-Management-System von ESET Remote Administrator können Sie ESET-Sicherheitslösungen auf Remotecomputern und Mobilgeräten installieren und schnell auf neue Probleme und Bedrohungen reagieren. ESET Remote Administrator bietet keinen Schutz vor Schadcode selbst, sondern stützt sich hierzu auf die auf jedem Client installierte ESET-Sicherheitslösung.

ESET-Sicherheitslösungen unterstützen Netzwerke, die verschiedene Plattformtypen umfassen. Ihr Netzwerk kann aus einer Kombination aktueller Microsoft-, Linux- und OS X-Betriebssysteme und Betriebssysteme für mobile Geräte (Mobiltelefone und Tablets) bestehen.

In der nachstehenden Abbildung sehen Sie eine Beispielarchitektur eines Netzwerks mit ESET-Sicherheitslösungen, die über ERA verwaltet werden:



HINWEIS: Weitere Informationen finden Sie in der ESET Remote Administrator-Onlinedokumentation.

2.1 ESET Remote Administrator-Server

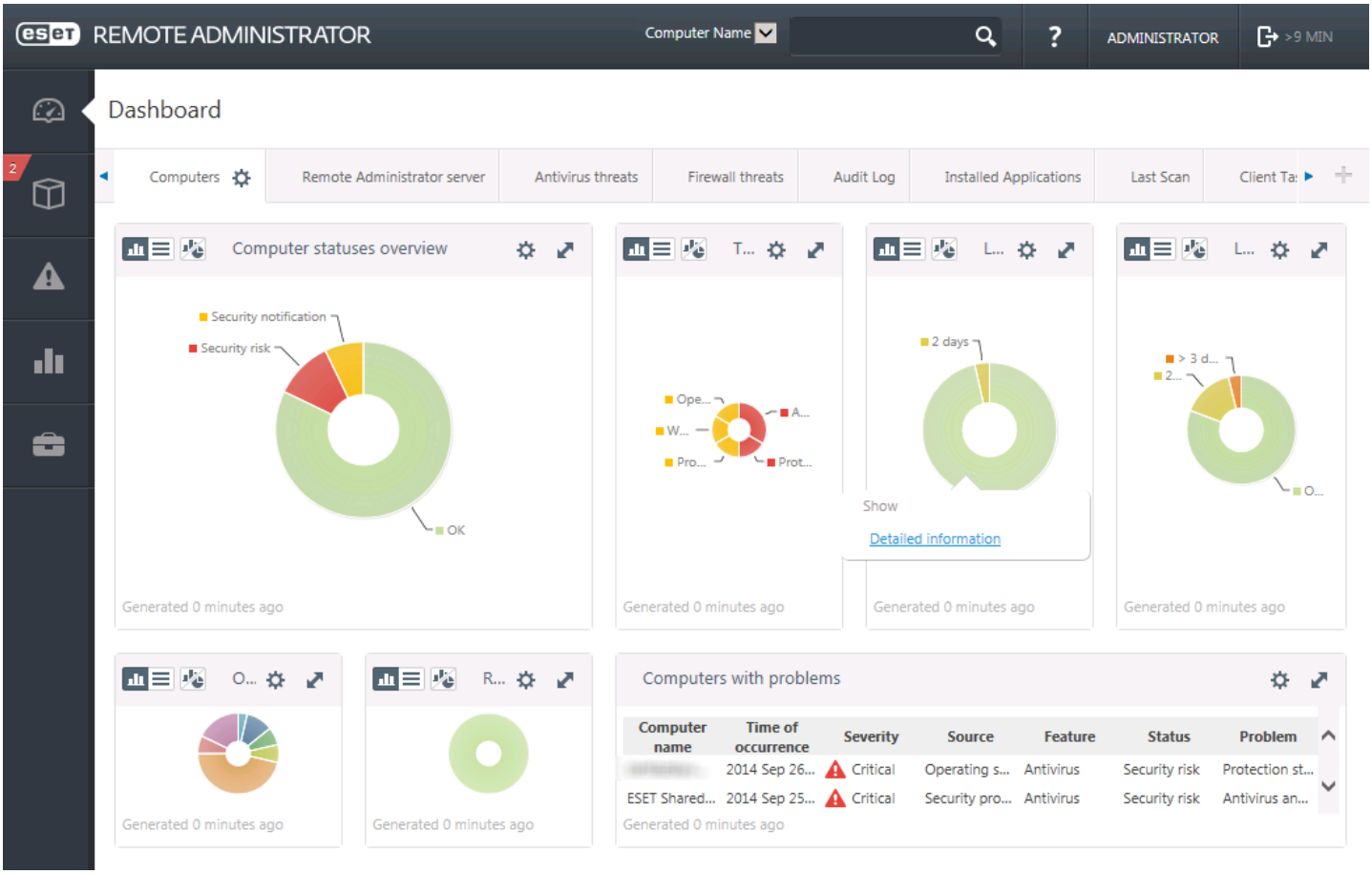
ESET Remote Administrator Server ist die ausführende Komponente von ESET Remote Administrator. Sie verarbeitet alle Daten von den Clients, die über den ESET-Agenten mit dem Server kommunizieren. Der ESET-Agent erleichtert die Kommunikation zwischen Client und Server. Daten wie Client-Logs, Konfigurationseinstellungen oder Agentreplikationen werden in einer Datenbank gespeichert, auf die ERA zum Zwecke der Berichterstellung zugreift.

Zur ordnungsgemäßen Verarbeitung der Daten benötigt der ERA-Server eine stabile Verbindung zum Datenbankserver. Zum Zwecke der Leistungsoptimierung wird empfohlen, den ERA-Server und die Datenbank auf separaten Servern zu installieren. Der Computer, auf dem der ERA-Server installiert wird, muss so konfiguriert sein, dass alle Agent-/Proxy-/RD Sensor-Verbindungen, welche anhand von Zertifikaten überprüft werden, akzeptiert werden. Nachdem der ERA-Server installiert ist, können Sie die ERA-Web-Konsole öffnen und Arbeitsstationen mit installierten ESET-Lösungen verwalten.

2.2 Web-Konsole

Die **ERA-Web-Konsole** ist eine webbasierte Benutzeroberfläche, in der Sie Daten vom ERA-Server anzeigen und die ESET-Sicherheitslösungen in Ihrem Netzwerk verwalten können. Der Zugriff auf die Web-Konsole erfolgt über einen Browser. Sie bietet eine Übersicht über den Status der Clients im Netzwerk und kann zur Remote-Bereitstellung von ESET-Lösungen auf unverwalteten Computern verwendet werden. Wahlweise können Sie den Zugriff über das Internet auf den Webserver zulassen. So können Sie ESET Remote Administrator von nahezu jedem beliebigen Standort und Gerät aus verwenden.

Dashboard der Web-Konsole:



Oben in der Web-Konsole befindet sich das **Schnellsuche**-Tool. Wählen Sie im Dropdownmenü entweder **Computername**, **IPv4-/IPv6-Adresse** oder **Bedrohungsname** aus und geben Sie im Textfeld eine Zeichenfolge für die Suche ein. Klicken Sie dann auf das Lupensymbol oder drücken Sie die **Eingabetaste**, um die Suche auszuführen. Sie werden zum Bereich **Gruppen** geleitet, wo das Suchergebnis angezeigt wird.

2.3 Proxy

Der **ERA-Proxy** ist ein weiterer Bestandteil von ESET Remote Administrator mit zwei Hauptzwecken. In einem mittelgroßen Netzwerk oder Unternehmensnetzwerk mit vielen Clients (beispielsweise 10.000 Clients oder mehr) können Sie mit einem ERA-Proxy die Last zwischen mehreren ERA-Proxys verteilen und so den primären ERA-Server entlasten. Sie können den ERA-Proxy außerdem für Verbindungen zu entfernt liegenden Büros mit schwacher Bandbreite einsetzen. In diesem Fall wird der ERA-Agent auf den Clients nicht direkt mit dem ERA-Hauptserver verbunden, sondern kommuniziert über den ERA-Proxy, der sich im gleichen lokalen Netzwerk wie der Client befindet. Diese Konfiguration reduziert die Last auf der Netzwerkverbindung zum Zweigstellenbüro. Der ERA-Proxy nimmt Verbindungen von allen lokalen ERA-Agenten an, kompiliert die empfangenen Daten und lädt sie zum primären ERA-Server (oder zu einem anderen ERA-Proxy) hoch. Auf diese Weise ist im Netzwerk Platz für mehr Clients, ohne dass die Leistungsfähigkeit des Netzwerks und der Datenbankabfragen beeinträchtigt wird.

Je nach Netzwerkkonfiguration kann ein ERA-Proxy eine Verbindung zu einem anderen ERA-Proxy und anschließend zum ERA-Server herstellen.

Damit der ERA-Proxy ordnungsgemäß funktioniert, muss auf dem Hostcomputer, auf dem sich der ERA-Proxy befindet, ein ESET-Agent installiert sein, und er muss mit der oberen Ebene (entweder dem ERA-Server oder, sofern vorhanden, dem oberen ERA-Proxy) des Netzwerks verbunden sein.

2.4 Agent

Der **ERA-Agent** ist eine wichtige Komponente von ESET Remote Administrator. Der Agent dient der Kommunikation zwischen den ESET-Sicherheitslösungen auf den Clientcomputern (z. B. ESET Endpoint Security) und dem ERA-Server. Dank dieser Kommunikation können Sie ESET-Sicherheitslösungen auf Remoteclients von einem zentralen Standort aus verwalten. Der Agent erfasst Informationen vom Client und sendet sie an den Server. Wenn der Server einen Task an einen Client sendet, wird der Task an den Agenten übermittelt, der wiederum mit dem Client kommuniziert. Der gesamte Netzwerkverkehr findet zwischen dem Agenten und dem oberen Teil des ERA-Netzwerks (Server und Proxy) statt.

Der ESET-Agent stellt mit einer der folgenden drei Methoden eine Verbindung zum Server her:

1. Der Agent des Client ist direkt mit dem Server verbunden.
2. Der Agent des Client ist über einen Proxy mit dem Server verbunden.
3. Der Agent des Client ist über mehrere Proxys mit dem Server verbunden.

Der ERA-Agent kommuniziert mit ESET-Lösungen auf einem Client, sammelt Daten aus Programmen auf diesem Client und leitet vom Server erhaltene Konfigurationsdaten an den Client weiter.

HINWEIS: Der ESET-Proxy verfügt über einen eigenen Agenten, der alle Kommunikationstasks zwischen Clients, anderen Proxys und dem ERA-Server abwickelt.

2.5 RD Sensor

RD (Rogue Detection) Sensor ist eine Komponente von ESET Remote Administrator, die das Netzwerk nach Computern durchsucht. Mit RD Sensor können Sie neue Computer ganz einfach zu ESET Remote Administrator hinzuzufügen, ohne sie manuell suchen und hinzufügen zu müssen. Jeder im Netzwerk gefundene Computer wird in der Web-Konsole angezeigt und der Standardgruppe „Alle“ hinzugefügt. Anschließend können Sie Aktionen an den einzelnen Clientcomputern durchführen.

RD Sensor ist ein passives Überwachungstool, das im Netzwerk vorhandene Computer erkennt und Informationen über diese Computer an den ERA-Server sendet. Der ERA-Server bewertet dann, ob die im Netzwerk gefundenen PCs unbekannt oder bereits verwaltet sind.

3. Remote-Installation

Für die Remote-Installation von ESET Endpoint Security über ERA ist Folgendes erforderlich:

- Installation des Connectors für Mobilgeräte
- Mobilgeräteregistrierung

Die Installation von ESET Endpoint Security kann auf zwei verschiedene Weisen ausgeführt werden:

1. Der Administrator sendet den Registrierungslink, die APK-Installationsdatei und eine kurze Installationsanweisung per E-Mail an die Endbenutzer. Wenn der Benutzer auf den Link tippt, wird der standardmäßige Internetbrowser auf dem Android-Gerät des Benutzers geöffnet und ESET Endpoint Security wird registriert und mit ERA verbunden. Wenn ESET Endpoint Security noch nicht auf dem Gerät installiert ist, wird der Benutzer automatisch zum Google Play Store weitergeleitet, um die App herunterzuladen. Anschließend wird eine Standardinstallation ausgeführt.
2. Der Administrator sendet die Anwendungseinstellungsdatei, die APK-Installationsdatei und eine kurze Installationsanweisung per E-Mail an die Endbenutzer. Alternativ können die Benutzer aufgefordert werden, die APK-Datei aus dem Google Play Store herunterzuladen. Der Administrator stellt den Link hierzu bereit. Nach der Installation öffnet der Benutzer die Anwendungseinstellungsdatei. Alle Einstellungen werden importiert und die Anwendung aktiviert (vorausgesetzt, die Lizenzinformationen wurden bereitgestellt).

4. Lokale Installation auf dem Gerät

ESET Endpoint Security bietet Administratoren die Möglichkeit, Endpoint lokal zu verwalten, wenn sie ESET Remote Administrator nicht verwenden möchten. Alle Anwendungseinstellungen werden mit dem Administratorpasswort geschützt, d. h. die Anwendung bleibt ständig unter vollständiger Kontrolle des Administrators.

Administratoren in kleineren Unternehmen, die ESET Remote Administrator nicht verwenden möchten, aber dennoch einen Schutz der Unternehmensgeräte implementieren und grundlegende Sicherheitsrichtlinien anwenden möchten, können die Geräte auf zwei Weisen lokal verwalten:

1. Physischer Zugriff auf jedes Unternehmensgerät und manuelle Konfiguration der Einstellungen.
2. Der Administrator kann die gewünschte Konfiguration auf dem eigenen Android-Gerät (mit installiertem ESET Endpoint Security) vorbereiten und diese Einstellungen in eine Datei exportieren. Weitere Informationen hierzu finden Sie im Abschnitt Einstellungen importieren/exportieren in diesem Handbuch. Der Administrator kann die exportierte Datei dann mit den Endbenutzern teilen, beispielsweise per E-Mail. Die Endbenutzer können diese Datei auf einem beliebigen Gerät, auf dem ESET Endpoint Security ausgeführt wird, importieren. Wenn der Benutzer die Einstellungsdatei öffnet und akzeptiert, werden automatisch alle Einstellungen importiert und die Anwendung aktiviert (sofern die Lizenzinformationen enthalten waren). Alle Einstellungen sind mit dem Administratorpasswort geschützt.

4.1 Download von der ESET-Website

Sie können ESET Endpoint Security herunterladen, indem Sie mit Ihrem Mobilgerät unter Verwendung einer QR-Scan-App den QR-Code unten einscannen:

Alternativ können Sie die APK-Installationsdatei für ESET Endpoint Security von der ESET-Website herunterladen:

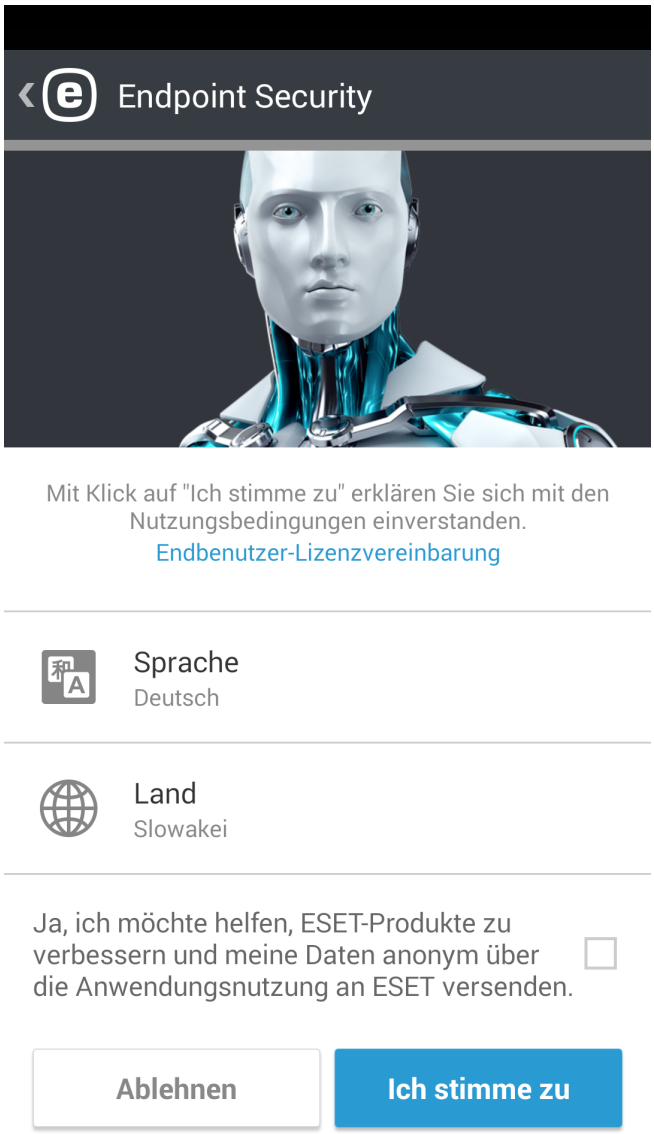
1. Laden Sie die Installationsdatei von der ESET-Website herunter.
2. Öffnen Sie die Datei aus dem Android-Benachrichtigungsbereich oder suchen Sie mit einer Dateibrowseranwendung nach ihr. Die Datei wird üblicherweise im Download-Ordner gespeichert.
3. Vergewissern Sie sich, dass Anwendungen aus unbekannten Quellen auf Ihrem Gerät zugelassen sind. Tippen Sie hierzu im Android-Startbildschirm auf das Symbol oder navigieren Sie zu **Start** > **Menü**. Tippen Sie auf **Einstellungen** > **Sicherheit**. Die Option **Unbekannte Quellen** muss zugelassen sein.
4. Öffnen Sie die Datei und tippen Sie auf **Installieren**.

4.2 Download aus Google Play

Öffnen Sie die Google Play Store-Anwendung auf Ihrem Android-Gerät und suchen Sie nach ESET Endpoint Security (oder nur „ESET“).

Alternativ können Sie das Programm auch herunterladen, indem Sie mit Ihrem Mobilgerät unter Verwendung einer QR-Scan-App den QR-Code unten einscannen:

4.3 Startassistent


Endpoint Security
Mit Klick auf "Ich stimme zu" erklären Sie sich mit den Nutzungsbedingungen einverstanden.
Endbenutzer-Lizenzvereinbarung
Sprache
Deutsch
Land
Slowakei
Ja, ich möchte helfen, ESET-Produkte zu verbessern und meine Daten anonym über die Anwendungsnutzung an ESET versenden.
Ablehnen
Ich stimme zu

Tippen Sie nach der Installation der Anwendung auf **Administratoreinrichtung** und befolgen Sie die Anweisungen des Startassistenten. Diese Prozedur sollte von Administratoren ausgeführt werden:

1. Wählen Sie die **Sprache** aus, die Sie in ESET Endpoint Security verwenden möchten.
2. Wählen Sie das **Land** aus, in dem Sie arbeiten oder leben.
3. Wenn Sie durch das Senden anonymer Daten über die Anwendungsnutzung zur Verbesserung der ESET-Produkte beitragen möchten, aktivieren Sie diese Option.
4. Tippen Sie auf **Ich stimme zu**. Damit stimmen Sie der Endbenutzer-Lizenzvereinbarung zu.
5. Wählen Sie aus, ob Sie ESET Endpoint Security mit ESET Remote Administrator verbinden oder eine manuelle Einrichtung ausführen möchten. Für Letzteres müssen Sie ein Administratorpasswort erstellen und den Deinstallationsschutz aktivieren.
6. Wählen Sie im nächsten Schritt aus, ob Sie an ESET Live Grid teilnehmen möchten. Weitere Informationen zu ESET Live Grid finden Sie in diesem Abschnitt.
7. Wählen Sie aus, ob ESET Endpoint Security eventuell unerwünschte Anwendungen erkennen soll. Weitere Informationen zu solchen Anwendungen finden Sie in diesem Abschnitt.
8. Aktivieren Sie das Produkt.

5. Deinstallation

Sie können ESET Endpoint Security mit dem Deinstallationsassistenten deinstallieren, den Sie unter **Einstellungen** > **Deinstallieren** im Hauptprogrammfenster aufrufen können. Wenn der Deinstallationsschutz aktiviert ist, werden Sie aufgefordert, das Administratorpasswort einzugeben.

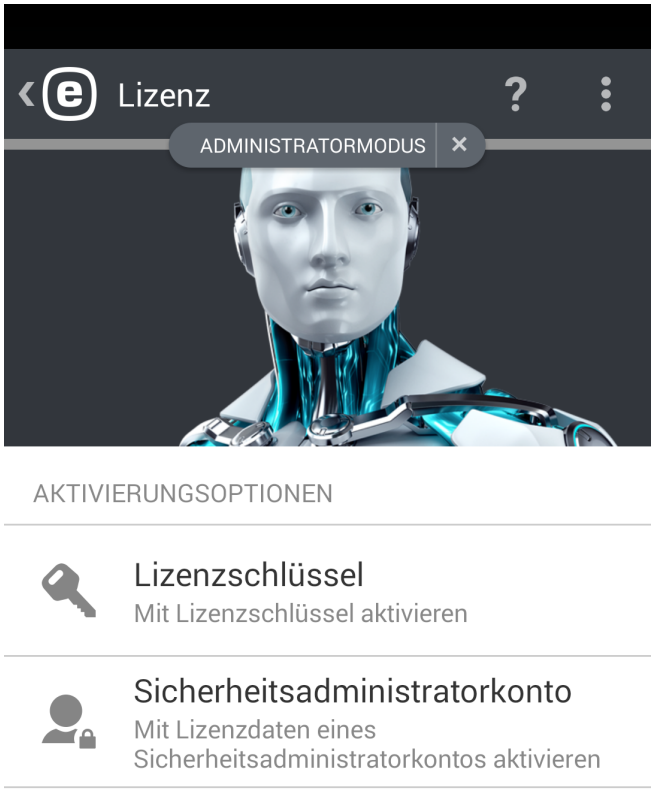
Alternativ können Sie das Produkt durch Ausführen folgender Schritte manuell deinstallieren:

1. Tippen Sie auf dem Android-Startbildschirm auf das Symbol (oder navigieren Sie zu **Start** > **Menü**) und tippen Sie auf **Einstellungen** > **Sicherheit** > **Geräteadministratoren**. Deaktivieren Sie ESET Endpoint Security und tippen Sie auf **Deaktivieren**. Tippen Sie auf **Entsperren** und geben Sie das Administratorpasswort ein. Wenn Sie ESET Endpoint Security nicht als Geräteadministrator eingerichtet haben, überspringen Sie diesen Schritt.
2. Kehren Sie zurück zur Option **Einstellungen** und tippen Sie auf **Apps verwalten** > ESET Endpoint Security > **Deinstallieren**.

6. Produktaktivierung

Es stehen mehrere Methoden zur Aktivierung von ESET Endpoint Security zur Verfügung. Die Verfügbarkeit einer bestimmten Aktivierungsmethode kann je nach Land und Vertriebsweg (ESET-Webseite usw.) des Produkts abweichen.

Um ESET Endpoint Security direkt auf dem Android-Gerät zu aktivieren, tippen Sie auf das Symbol **Menü** im Hauptbildschirm von ESET Endpoint Security (oder drücken Sie die Taste **MENÜ** auf dem Gerät). Tippen Sie dann auf **Lizenz**.



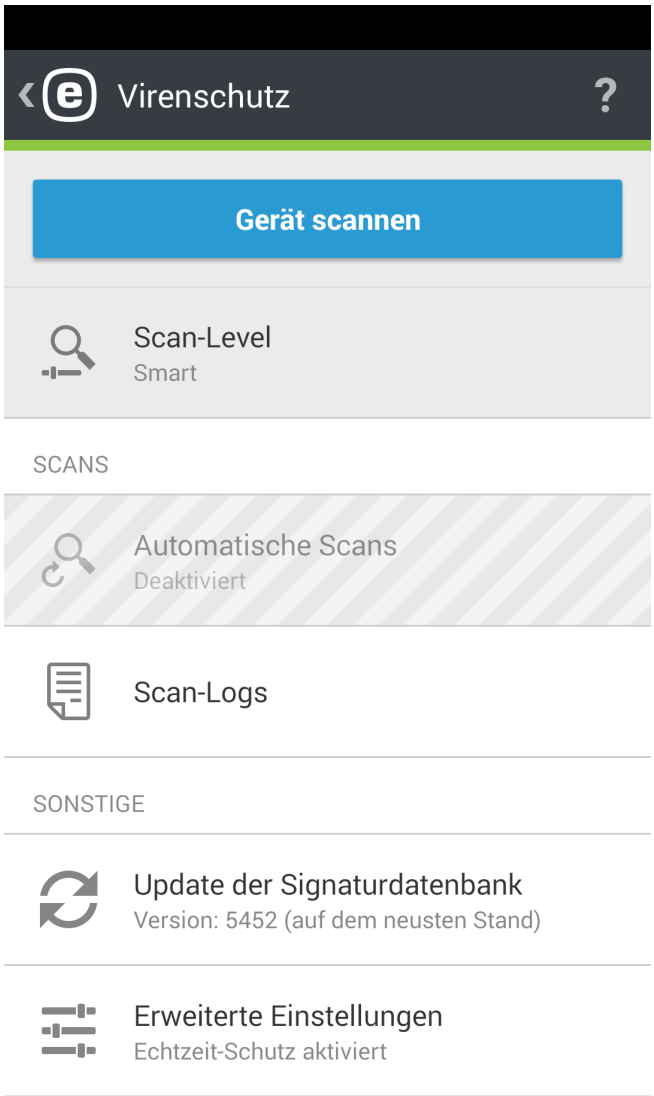
Sie können ESET Endpoint Security mit einer der folgenden Methoden aktivieren:

- **Lizenzschlüssel** - eine eindeutige Zeichenkette im Format XXXX-XXXX-XXXX-XXXX-XXXX, die zur Identifizierung des Lizenzinhabers und zur Aktivierung der Lizenz verwendet wird.
- **Sicherheitsadministratorkonto** - ein im ESET License Administrator-Portal erstelltes Konto mit Anmeldedaten (E-Mail-Adresse und Passwort). Mit dieser Methode können Sie mehrere Lizenzen von einem Standort aus verwalten.

HINWEIS: ESET Remote Administrator kann Clientgeräte mithilfe von Lizenzen, die der Administrator bereitstellt, im Hintergrund aktivieren.

7. Virenschutz

Das Virenschutzmodul schützt Ihr Gerät vor Schadcode, indem es Bedrohungen blockiert und säubert oder in die Quarantäne verschiebt.



Gerät scannen

Mit der Funktion „Gerät scannen“ können Sie Ihr Gerät auf eingedrungenen Schadcode prüfen.

Bestimmte vordefinierte Dateitypen werden standardmäßig gescannt. Bei einem vollständigen Gerätescan werden der Speicher, ausgeführte Prozesse und ihre abhängigen DLLs und Dateien des internen Speichers und Wechselspeichers geprüft. Eine kurze Zusammenfassung des Scans wird in einer Log-Datei gespeichert, die im Bereich „Scan-Logs“ verfügbar ist.

Wenn Sie einen bereits ausgeführten Scan abbrechen möchten, tippen Sie auf das Symbol .

Scan-Stufe

Sie können aus zwei verschiedenen Scan-Stufen auswählen:

- **Smart** - Beim Smart-Scan werden installierte Anwendungen, DEX-Dateien (ausführbare Dateien des Android-Betriebssystems), SO-Dateien (Bibliotheken) und ZIP-Dateien mit einer maximalen Scan-Tiefe von 3 verschachtelten Archive und der SD-Karteninhalt gescannt.
- **Tiefen-Scan** - Alle Dateitypen im internen Speicher und auf der SD-Karte werden unabhängig von der Dateierweiterung gescannt.

Automatische Scans

Zusätzlich zu den On-Demand-Scans können mit ESET Endpoint Security auch automatische Scans ausgeführt werden. Informationen zum Scannen beim Laden und zu geplanten Scans finden Sie in diesem Abschnitt.

Scan-Logs

Der Bereich „Scan-Logs“ enthält umfangreiche Daten zu abgeschlossenen Scans in Form von Log-Dateien. Weitere Informationen finden Sie im Abschnitt Virenschutz-Scan-Logs in diesem Dokument.

Update der Signaturdatenbank

Standardmäßig enthält ESET Endpoint Security einen Update-Task, um sicherzustellen, dass das Programm regelmäßig aktualisiert wird. Um manuell ein Update auszuführen, tippen Sie auf **Update der Signaturdatenbank**.

HINWEIS: Um eine unnötige Ausnutzung der Bandbreite zu vermeiden, werden Updates je nach Bedarf beim Hinzufügen einer neuen Bedrohung veröffentlicht. Mit einer aktiven Lizenz sind Updates kostenlos. Ihr Mobildienstanbieter berechnet jedoch möglicherweise Gebühren für die Datenübertragung.

Eine ausführliche Beschreibung der erweiterten Einstellungen des Virenschutzes finden Sie im Abschnitt Erweiterte Einstellungen in diesem Dokument.

7.1 Automatische Scans

Scan-Stufe

Sie können aus zwei verschiedenen Scan-Stufen auswählen. Diese Einstellung gilt für Scans während des Ladevorgangs und für geplante Scans:

- **Smart** - Beim Smart-Scan werden installierte Anwendungen, DEX-Dateien (ausführbare Dateien des Android-Betriebssystems), SO-Dateien (Bibliotheken) und ZIP-Dateien mit einer maximalen Scan-Tiefe von 3 verschachtelten Archive und der SD-Karteninhalt gescannt.
- **Tiefen-Scan** - Alle Dateitypen im internen Speicher und auf der SD-Karte werden unabhängig von der Dateierweiterung gescannt.

Scan während Ladevorgang

Wenn diese Option aktiviert ist, wird der Scan automatisch gestartet, sobald das Gerät im Ruhezustand (vollständig geladen und an ein Ladegerät angeschlossen) ist.

Geplanter Scan

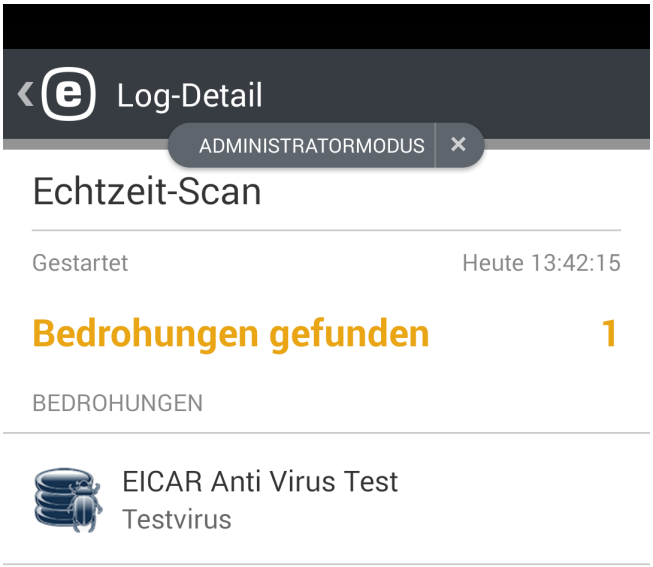
Mithilfe eines geplanten Scans können Sie einen Geräte-Scan zu einer vordefinierten Zeit ausführen lassen. Um einen Scan zu planen, tippen Sie auf neben **Geplanter Scan** und geben Sie die Uhrzeit und Daten an, zu denen der Scan gestartet werden soll. Standardmäßig ist „Montag“ und „04:00 Uhr“ eingestellt.

7.2 Scan-Logs

Scan-Logs werden nach jedem geplanten Scan und jedem manuell ausgelösten Geräte-Scan erstellt.

Jedes Log enthält folgende Informationen:

- Datum und Uhrzeit des Ereignisses
- Dauer des Scans
- Anzahl der gescannten Dateien
- Scan-Ergebnis oder während dem Scan aufgetretene Fehler



7.3 Erweiterte Einstellungen

Echtzeit-Schutz

Mit dieser Option können Sie den Echtzeit-Scanner aktivieren oder deaktivieren. Dieser Scanner wird beim Systemstart automatisch gestartet und scannt die Dateien, die Sie verwenden. Er scannt automatisch den Download-Ordner, die APK-Installationsdateien und die Dateien auf der SD-Karte, sobald diese eingehängt ist.

ESET Live Grid

ESET Live Grid bietet Ihnen auf der Grundlage des leistungsfähigen ThreatSense.net-Frühwarnsystems zusätzlichen Schutz für Ihr Gerät. Es überwacht laufend die ausgeführten Programme und Prozesse auf Ihrem System und überprüft sie anhand aktueller Informationen, die uns von Millionen ESET-Anwendern weltweit bereitgestellt werden. Da die ESET Live Grid-Datenbank mit der Zeit wächst, werden die Scans außerdem schneller und die Erkennungsgenauigkeit erhöht sich. So können wir allen ESET-Benutzern einen schnelleren und besseren Schutz bieten. Wir empfehlen, diese Funktion zu aktivieren, und bedanken uns für Ihre Unterstützung.

Evtl unerwünschte Anwendungen erkennen

Eine unerwünschte Anwendung ist ein Programm, das Adware enthält, Toolbars installiert, ihre Suchergebnisse verfolgt oder andere unklare Ziele hat. In manchen Fällen können Sie der Meinung sein, dass die Vorteile der unerwünschten Anwendung bedeutender sind als die Risiken. Aus diesem Grund weist ESET solchen Anwendungen eine niedrigere Risikoeinstufung zu als anderen Schadcodearten.

Potenziell unsichere Anwendungen erkennen

Es gibt zahlreiche seriöse Anwendungen, die die Verwaltung miteinander vernetzter Geräte vereinfachen sollen. Diese Programme können jedoch auch für schädliche Zwecke missbraucht werden. Mit der Option „Potenziell unsichere Anwendungen erkennen“ können Sie diese Art Anwendung überwachen und je nach Wunsch blockieren. Zur Kategorie der *Potenziell unsicheren Anwendungen* zählen Programme, die zwar erwünscht sind, jedoch potenziell gefährliche Funktionen bereitstellen. Diese Kategorie umfasst Programme wie Remotezugriffstools, Anwendungen zum Entschlüsseln von Passwörtern und Keylogger.

Unaufgelöste Bedrohungen blockieren

Diese Einstellung bestimmt, welche Aktion ausgeführt werden soll, wenn die Prüfung abgeschlossen ist und Bedrohungen gefunden wurden. Wenn Sie diese Option aktivieren, kann die infizierte Datei nicht mehr ausgeführt werden.

Updates der Signaturdatenbank

Hier können Sie das Zeitintervall festlegen, in dem die Updates der Signaturdatenbank automatisch heruntergeladen werden. Die Updates werden nach Bedarf veröffentlicht, wenn eine neue Bedrohung zur Datenbank hinzugefügt wurde. Wir empfehlen, den Standardwert (täglich) für diese Option aktiviert zu lassen.

Benutzerdefiniertes maximales Datenbankalter

Standardmäßig erneuert ESET Endpoint Security die Signaturdatenbank alle 7 Tage, wenn kein Update ausgegeben wird.

Update-Server

Über diese Option können Sie Ihr Gerät wahlweise über den **Testserver** aktualisieren. Test-Updates wurden intern umfassend geprüft und werden demnächst veröffentlicht. Wenn Sie den Testmodus aktivieren, können Sie früher von den neuesten Erkennungsmethoden und Fehlerkorrekturen profitieren. Test-Updates sind jedoch nicht immer stabil. Eine Liste der aktuellen Module finden Sie im Abschnitt **Über**: Tippen Sie im Hauptbildschirm von ESET Endpoint Security auf das Menüsymbol und tippen Sie auf **Über** > ESET Endpoint Security. Es wird empfohlen, die Option **Release-Server** aktiviert zu lassen (Standard).

bietet die Möglichkeit, Kopien der Update-Dateien zu erstellen. Diese können Sie dann zur Aktualisierung anderer Geräte im Netzwerk verwenden. Einsatz eines **lokalen Mirrors** - das Vorhalten von Kopien der Update-Dateien im lokalen Netzwerk - kann vorteilhaft sein, da die Dateien dann nicht von allen mobilen Geräten einzeln über das Internet heruntergeladen werden müssen. Ausführliche Informationen zum Konfigurieren des Mirror-Servers mithilfe der ESET Endpoint-Produkte für Windows finden Sie in diesem Dokument.

8. Anti-Theft

Die **Anti-Theft**-Funktion schützt Ihr Mobilgerät vor unbefugtem Zugriff.

Wenn Ihr Gerät verloren geht oder gestohlen wird und jemand die SIM-Karte durch eine neue (nicht vertrauenswürdige) Karte ersetzt, wird das Gerät von ESET Endpoint Security automatisch gesperrt und an die benutzerdefinierten Telefonnummern wird eine SMS-Warnnachricht gesendet. Die Nachricht enthält die Telefonnummer der aktuell eingelegten SIM-Karte, die IMSI-Nummer (International Mobile Subscriber Identity) und die IMEI-Nummer (International Mobile Equipment Identity) des Telefons. Der nicht autorisierte Benutzer weiß nicht, dass diese Meldung gesendet wurde, da sie automatisch aus den Nachrichtenlisten auf dem Gerät gelöscht wird. Sie können außerdem die GPS-Koordinaten des verlorenen Mobilgeräts anfordern oder remote alle auf dem Gerät gespeicherten Daten löschen.

HINWEIS: Bestimmte Anti-Theft-Funktionen (vertrauenswürdige SIM-Karten und SMS-Textbefehle) sind auf Tablets ohne Messaging-Unterstützung nicht verfügbar.

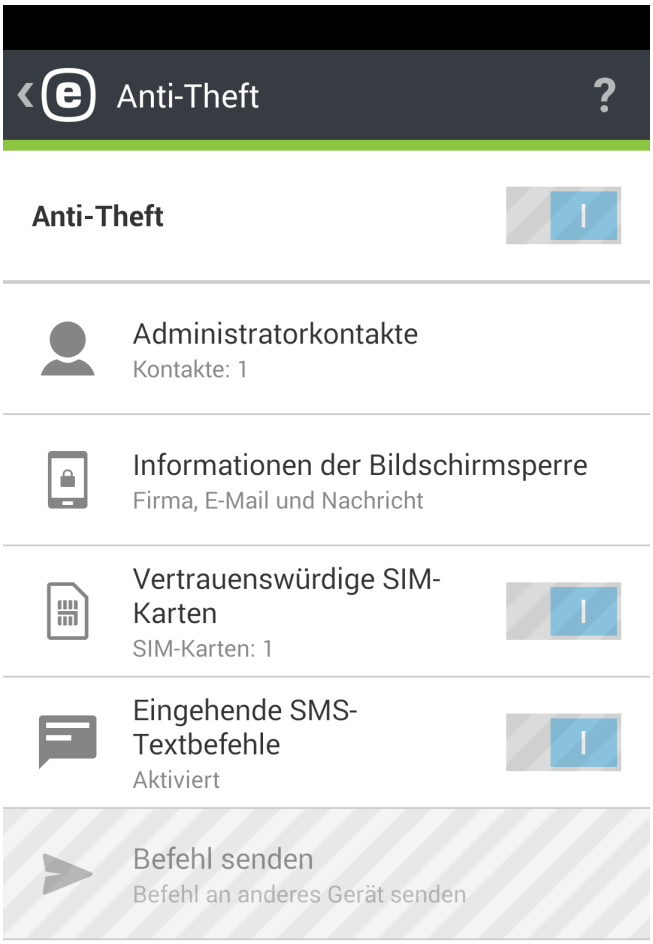
Anti-Theft-Funktionen helfen Administratoren, vermisste Geräte zu schützen und ihren Standort zu ermitteln. Die Aktionen können von ERA oder über SMS-Befehle ausgelöst werden.

In ESET Endpoint Security 2 können die gleichen SMS-Befehle wie in Version 1 verwendet werden (Sperren, Daten löschen und Orten). Zusätzlich sind folgende neue Befehle verfügbar:

- **Entsperren** – entsperrt das gesperrte Gerät.
- **Erweitertes Zurücksetzen auf Werkseinstellungen** - Alle zugreifbaren Daten auf dem Gerät werden schnell gelöscht (Dateikopfdaten werden zerstört) und das Gerät wird auf die standardmäßigen Werkseinstellungen zurückgesetzt.
- **Sirene** - Das vermisste Gerät wird gesperrt und gibt einen sehr lauten Ton wider, selbst wenn es stumm geschaltet ist.

Um die Sicherheit der SMS-Befehle zu erhöhen, empfängt der Administrator auf seinem Mobilgerät (unter der in der Administratorkontaktliste festgelegten Nummer) einen eindeutigen und zeitlich begrenzt gültigen SMS-Überprüfungscode, wenn er einen SMS-Befehl ausführt. Dieser Überprüfungscode wird zur Überprüfung eines bestimmten Befehls verwendet.

Wenn ein Administrator beispielsweise eine SMS mit dem Inhalt *eset lock* an ein verwaltetes Gerät (zum Beispiel ein verlorenes Mobiltelefon) sendet, erhält er eine SMS mit einem Überprüfungscode für diesen Befehl. Der Administrator sendet dann eine neue SMS an die gleiche Telefonnummer, die den Text *eset lock*, gefolgt vom Überprüfungscode, enthält. Daraufhin wird der Befehl überprüft und ausgeführt. SMS-Befehle können von einem beliebigen Mobiltelefon und einer beliebigen, in den Administratorkontakten enthaltenen Telefonnummer aus gesendet werden.



Beim Ausführen von Befehlen per SMS empfängt der Administrator eine SMS, die bestätigt, dass der Befehl gesendet wurde. Beim Ausführen von Befehlen von ERA wird in ERA eine Bestätigung angezeigt.

Wenn Standortinformationen (Suchbefehl) empfangen werden, werden diese in ESET Remote Administrator in Form von GPS-Koordinaten angezeigt. Wenn der Befehl über SMS ausgeführt wurde, werden die Standortinformationen (GPS-Koordinaten und ein Link zu Google Maps) per SMS empfangen. Wenn die SMS-Befehle über die grafische Benutzeroberfläche gesendet werden (Funktion **Befehl senden**), werden die empfangenen Informationen in der spezifischen grafischen Benutzeroberfläche angezeigt.

Alle Anti-Theft-Befehle können auch in ERA ausgeführt werden. Dank der neuen Funktion für die Mobilgeräteverwaltung kann der Administrator Anti-Theft-Befehle mit nur wenigen Clicks ausführen. Die Tasks werden mit einer neuen Verarbeitungskomponente für Push-Befehle (Connector für Mobilgeräte), die nun Bestandteil der ERA-Infrastruktur ist, sofort zur Ausführung eingereicht.

8.1 Administratorkontakte

Dies ist die Liste der Administrator-Telefonnummern, die durch ein Administratorpasswort geschützt ist. Anti-Theft-Befehle können nur von vertrauenswürdigen Nummern aus gesendet werden. An diese Nummern werden auch die Benachrichtigungen zu Anti-Theft-Aktionen gesendet.

8.1.1 Hinzufügen eines Administratorkontakts

Im Einrichtungsassistenten für Anti-Theft sollten der Name und eine Telefonnummer eines Administrators angegeben werden. Wenn der Kontakt mehrere Telefonnummern enthält, werden alle verknüpften Nummern berücksichtigt.

Sie können Administratorkontakte über den Bereich **Anti-Theft** > **Administratorkontakte** hinzufügen.

8.2 Informationen der Bildschirmsperre

Der Administrator kann benutzerdefinierte Informationen (Firmenname, E-Mail-Adresse, Nachricht) festlegen, die angezeigt werden, wenn das Gerät gesperrt ist. Außerdem kann er festlegen, dass vordefinierte Administratorkontakte angerufen werden können.

Diese Informationen umfassen Folgendes:

- Firmenname (optional)
- E-Mail-Adresse (optional)
- Benutzerdefinierte Nachricht

8.3 Vertrauenswürdige SIM-Karten

Im Bereich **Vertrauenswürdige SIM-Karte** enthält die Liste der vertrauenswürdigen SIM-Karten, die von ESET Endpoint Security akzeptiert werden. Wenn Sie eine SIM-Karte einlegen, die nicht in dieser Liste enthalten sind, wird der Bildschirm gesperrt und der Administrator enthält eine SMS-Warnnachricht.

Um eine neue SIM-Karte hinzuzufügen, tippen Sie auf das Symbol ✚. Geben Sie im Feld **Name** einen Namen für die SIM-Karte (beispielsweise „Privat“ oder „Geschäftlich“) und geben Sie die IMSI (International Mobile Subscriber Identity)-Nummer ein. Die IMSI ist üblicherweise eine 15-stellige Nummer, die direkt auf der SIM-Karte aufgedruckt ist. In einigen Fällen kann die IMSI auch kürzer sein.

Um eine SIM-Karte aus der Liste zu entfernen, berühren und halten Sie den Eintrag und tippen Sie dann auf das Symbol 🗑.

HINWEIS: Die Funktion der vertrauenswürdigen SIM-Karten ist auf CDMA-, WCDMA- und Nur-WLAN-Geräten nicht verfügbar.

8.4 Remotebefehle

Remotebefehle können auf drei verschiedene Arten ausgelöst werden:

- direkt über die ERA-Konsole
- mit der Funktion **Befehl senden** in ESET Endpoint Security auf dem Android-Gerät des Administrators
- durch Senden von SMS-Textmeldungen vom Gerät des Administrators

Damit Administratoren, die nicht ERA verwenden, auf einfache Weise SMS-Befehle ausführen können, können diese Befehle über eine auf dem Android-Gerät des Administrators installierte Instanz von ESET Endpoint Security ausgelöst werden. Statt die Textmeldung manuell einzugeben und mit dem Überprüfungscode zu bestätigen, kann der Administrator auch die Funktion **Befehl senden** (nur im Administratormodus verfügbar) verwenden. Dazu gibt der Administrator die Telefonnummer ein oder wählt eine in den Kontakten gespeicherte Nummer aus und wählt dann im Dropdown-Menü den Sendebefehl aus. ESET Endpoint Security führt daraufhin alle erforderlichen Schritte ohne weitere Benutzerinteraktion im Hintergrund aus.

Zum Senden von SMS-Befehlen muss die Telefonnummer des Administrators auf dem Zielgerät als Administratorkontact gespeichert sein. Der Administrator erhält einen Überprüfungscode, der eine Stunde lang gültig ist und zum Ausführen beliebiger der nachstehenden Befehle verwendet werden kann. Der Code muss an die Nachricht angehängt werden, die den Befehl enthält. Dabei ist folgendes Format einzuhalten: `eset find Code`. Der Administrator empfängt eine Bestätigung, nachdem der Befehl auf dem Zielgerät ausgeführt wurde. Die folgenden SMS-Befehle können gesendet werden:

Orten
SMS-Befehl: `eset find`
Sie erhalten eine Textnachricht mit den GPS-Koordinaten des Zielgeräts und einem Link zu diesem Standort in Google Maps. Wenn nach 10 Minuten eine genauere Standortangabe verfügbar ist, sendet das Gerät eine neue SMS.

Sperren
SMS-Befehl: `eset lock`
Mit diesem Befehl wird das Gerät gesperrt. Sie können es mit dem Administratorpasswort oder dem Remotebefehl „Entsperren“ wieder entsperren. Wenn Sie diesen Befehl per SMS senden, können Sie eine benutzerdefinierte Nachricht anhängen, die auf dem Bildschirm des gesperrten Geräts angezeigt wird. Verwenden Sie hierzu folgendes Format: `eset lock Code Nachricht`. Wenn Sie den Parameter für die Nachricht leer lassen, wird eine Meldung aus dem Abschnitt Informationen der Bildschirmsperre angezeigt.

Entsperren
SMS-Befehl: `eset unlock`
Das Gerät wird entsperrt und die aktuell eingelegte SIM-Karte wird als vertrauenswürdige SIM-Karte gespeichert.

Alarmsirene
SMS-Befehl: `eset siren`
Eine laute Alarmsirene wird aktiviert, auch wenn das Gerät stummgeschaltet ist.

Erweitertes Zurücksetzen auf Werkseinstellungen
SMS-Befehl: `eset enhanced factory reset`
Das Gerät wird auf die Werkseinstellungen zurückgesetzt. Alle zugreifbaren Daten werden gelöscht und die Dateiköpfe werden entfernt. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.

Daten löschen
SMS-Befehl: `eset wipe`
Alle Kontakte, Nachrichten, E-Mails, Konten, Inhalte der SD-Karte, Bilder, Musik- und Videodaten, die in den standardmäßigen Ordnern gespeichert sind, werden dauerhaft vom Gerät gelöscht. ESET Endpoint Security bleibt auf dem Gerät installiert.

HINWEIS: Groß- und Kleinschreibung ist für SMS-Befehle nicht relevant.

9. Anwendungskontrolle

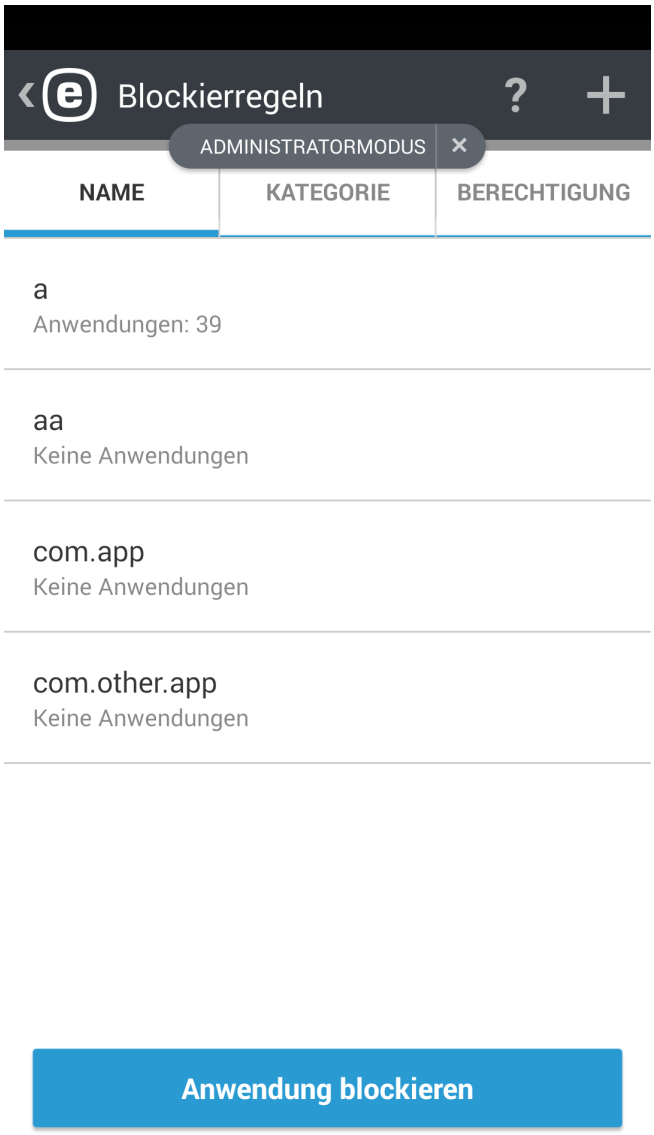
Die Funktion **Anwendungskontrolle** bietet Administratoren die Möglichkeit, installierte Anwendungen zu überwachen, den Zugriff auf gesperrte Anwendungen zu unterbinden und das Gefahrenrisiko zu senken, indem Benutzer zur Deinstallation bestimmter Anwendungen aufgefordert werden. Dem Administrator stehen verschiedene Filtermethoden für die Anwendungen zur Verfügung:

- Manuelles Festlegen der zu blockierenden Anwendungen
- Kategoriebasiertes Blockieren (zum Beispiel Spiele oder soziale Medien)
- Berechtigungsbasiertes Blockieren (zum Beispiel Anwendungen, die den Standort verfolgen)
- Blockieren nach Quelle (zum Beispiel Anwendungen, die aus anderen Quellen als dem Google Play Store stammen)

9.1 Blockierregeln

Im Bereich **Anwendungskontrolle** > **Blockieren** > **Blockierregeln** können Sie Regeln zum Blockieren von Anwendungen erstellen. Folgende Kriterien stehen zur Auswahl:

- Anwendungs- oder Paketname
- Kategorie
- Berechtigungen



9.1.1 Nach Anwendungsname blockieren

Mit ESET Endpoint Security können Administratoren Anwendungen auf Grundlage ihres Namens oder des Paketnamens blockieren. Im Bereich **Blockierregeln** wird eine Übersicht der erstellten Regeln und eine Liste der blockierten Anwendungen angezeigt.

Um eine vorhandene Regel zu ändern, berühren und halten Sie die Regel berührt und tippen Sie dann auf **Bearbeiten** . Um Regeleinträge aus der Liste zu entfernen, berühren Sie einen Eintrag und halten Sie ihn gedrückt. Wählen Sie die zu entfernenden Regeln aus und tippen Sie auf **Entfernen** . Um die gesamte Liste zu löschen, tippen Sie auf **ALLE AUSWÄHLEN** und dann auf **Entfernen** .

Wenn Sie eine Anwendung nach Name blockieren, sucht ESET Endpoint Security nach einer genauen Übereinstimmung mit dem Namen einer gestarteten Anwendung. Wenn Sie die grafische Benutzeroberfläche von ESET Endpoint Security in eine andere Sprache umstellen, müssen Sie den Anwendungsnamen in der neuen Sprache eingeben, damit die Anwendung weiterhin blockiert wird.

Um Probleme mit lokalisierten Anwendungsnamen zu vermeiden, empfiehlt es sich, solche Anwendungen nach ihrem Paketnamen zu blockieren. Der Paketname ist eine eindeutige Anwendungsidentifizierung, die während der Laufzeit nicht geändert und nicht von einer anderen Anwendung wiederverwendet werden kann.

Im Falle eines lokalen Administrators kann der Benutzer die Anwendungspaketnamen unter **Anwendungssteuerung** > **Überwachung** > **Zugelassene Anwendungen** finden. Nachdem auf eine Anwendung getippt wurde, wird der Bildschirm **Detail** mit dem Anwendungspaketnamen angezeigt. Um eine Anwendung zu blockieren, führen Sie diese Schritte aus.

9.1.1.1 So blockieren Sie Anwendungen auf Grundlage des Anwendungsnamens

1. Tippen Sie auf **Anwendungskontrolle** > **Blockieren** > **Anwendungen blockieren** > **Nach Namen blockieren**.
2. Wählen Sie aus, ob die Anwendung auf Grundlage des Anwendungs- oder des Paketnamens blockiert werden soll.
3. Geben Sie die Filterwörter ein, auf deren Grundlage die Anwendung blockiert werden soll. Verwenden Sie ein Komma (,) als Trennzeichen zwischen Wörtern.

Wenn Sie beispielsweise das Wort „*poker*“ im Feld **Anwendungsname** eingeben, werden alle Anwendungen blockiert, deren Name das Wort „*poker*“ enthält. Wenn Sie „*com.poker.game*“ in das Feld **Paketname** eingeben, blockiert ESET Endpoint Security nur eine Anwendung.

9.1.2 Blockieren nach Anwendungskategorie

Mit ESET Endpoint Security können Administratoren Anwendungen auf Grundlage vordefinierter Anwendungskategorien blockieren. Im Bereich **Blockierregeln** wird eine Übersicht der erstellten Regeln und eine Liste der blockierten Anwendungen angezeigt.

Wenn Sie eine bestehende Regel ändern möchten, berühren Sie die Regel, halten Sie sie gedrückt und tippen Sie auf **Bearbeiten** .

Um Regeleinträge aus der Liste zu entfernen, berühren Sie einen Eintrag und halten Sie ihn gedrückt. Wählen Sie die zu entfernenden Regeln aus und tippen Sie auf **Entfernen** . Um die gesamte Liste zu löschen, tippen Sie auf **ALLE AUSWÄHLEN**.

9.1.2.1 Blockieren einer Anwendung auf Grundlage der Anwendungskategorie

1. Tippen Sie auf **Anwendungskontrolle** > **Blockieren** > **Anwendungen blockieren** > **Nach Kategorie blockieren**.
2. Wählen Sie über die Kontrollkästchen vordefinierte Kategorien aus und tippen Sie auf **Blockieren**.

9.1.3 Blockieren nach Anwendungsberechtigungen

Mit ESET Endpoint Security können Administratoren Anwendungen auf Grundlage der Anwendungsberechtigungen blockieren. Im Bereich **Blockierregeln** wird eine Übersicht der erstellten Regeln und eine Liste der blockierten Anwendungen angezeigt.

Wenn Sie eine bestehende Regel ändern möchten, berühren Sie die Regel, halten Sie sie gedrückt und tippen Sie auf **Bearbeiten** .

Um Regeleinträge aus der Liste zu entfernen, berühren Sie einen Eintrag und halten Sie ihn gedrückt. Wählen Sie die zu entfernenden Regeln aus und tippen Sie auf **Entfernen** . Um die gesamte Liste zu löschen, tippen Sie auf **ALLE AUSWÄHLEN**.

9.1.3.1 So blockieren Sie Anwendungen auf Grundlage der Anwendungsberechtigungen

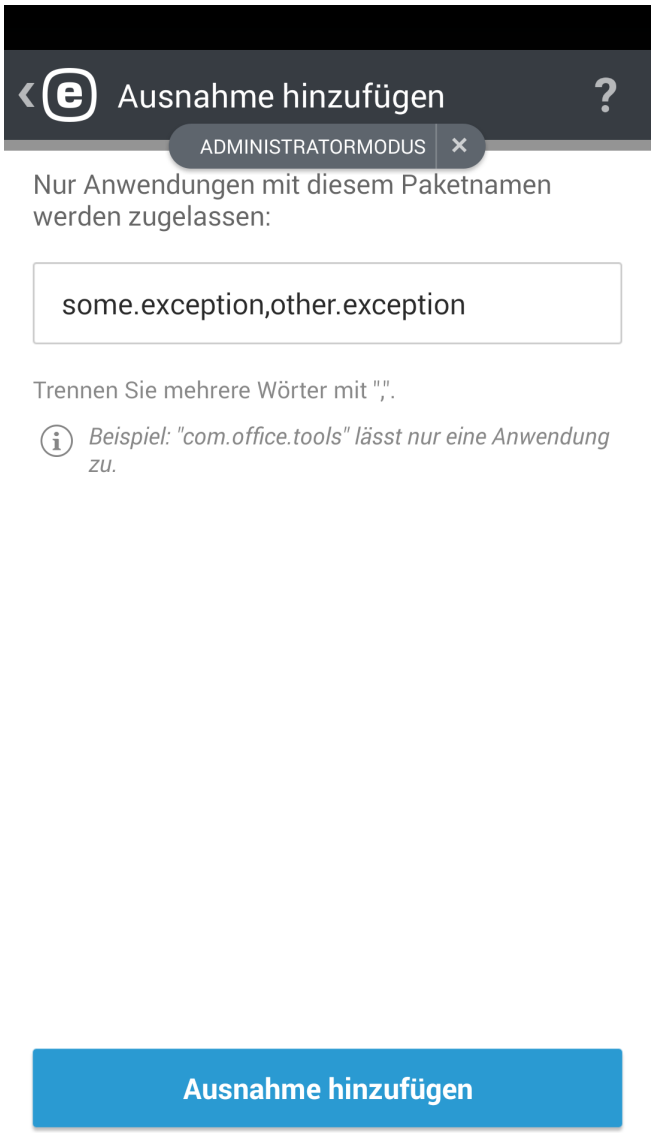
1. Tippen Sie auf **Anwendungskontrolle** > **Blockieren** > **Anwendungen blockieren** > **Nach Berechtigung blockieren**.
2. Wählen Sie über die Kontrollkästchen Berechtigungen aus und tippen Sie auf **Blockieren**.

9.1.4 Unbekannte Quellen blockieren

Standardmäßig blockiert ESET Endpoint Security keine Anwendungen, die aus dem Internet oder anderen Quellen als dem Google Play Store stammen. Im Bereich **Blockierte Anwendungen** wird eine Übersicht der blockierten Anwendungen (Paketname, angewendete Regel) angezeigt. Außerdem haben Sie hier die Möglichkeit, eine blockierte Anwendung zu deinstallieren oder zum Bereich **Ausnahmen** (Positivliste) hinzuzufügen.

9.2 Ausnahmen

Sie können Ausnahmen festlegen, um bestimmte Anwendungen von der Liste gesperrter Anwendungen auszuschließen. Administratoren, die ESET Endpoint Security remote verwalten, können mithilfe dieser Funktion ermitteln, ob ein bestimmtes Gerät die Unternehmensrichtlinien in Bezug auf installierte Anwendungen erfüllt.

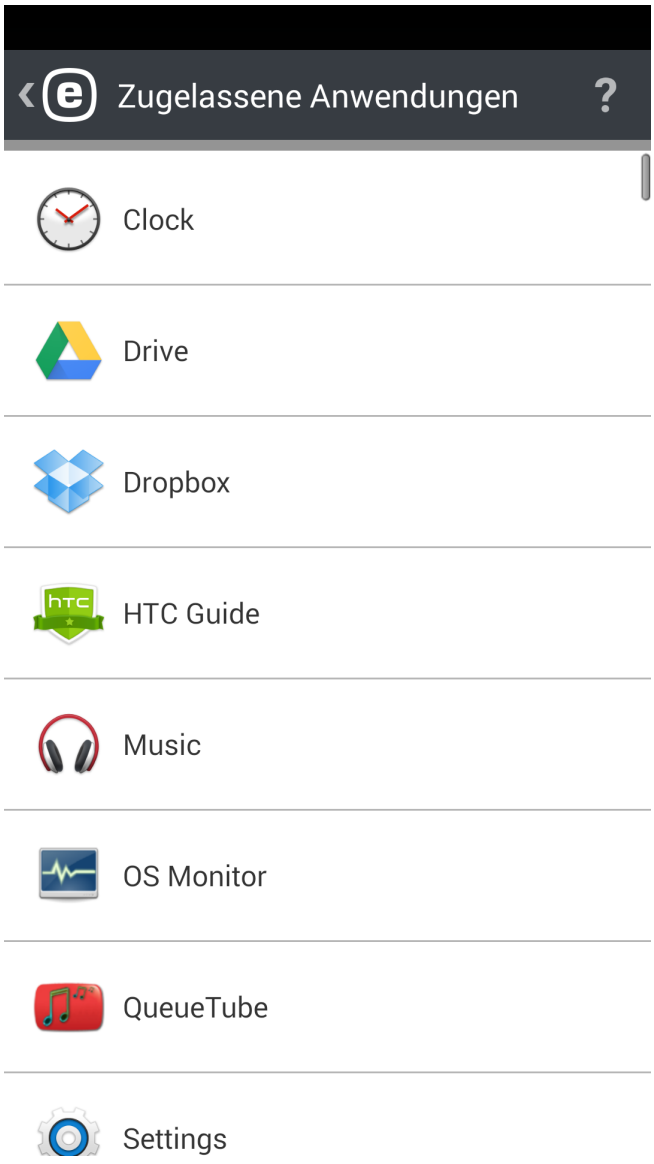


9.2.1 Hinzufügen von Ausnahmen

Anwendungen können durch Hinzufügen einer neuen Ausnahme (Eingabe des Paketnamens der Anwendung) oder durch Ausschluss aus der Liste **Blockierte Anwendungen** in die Positivliste aufgenommen werden.

9.3 Zugelassene Anwendungen

Dieser Bereich enthält eine Übersicht über die installierten Anwendungen, die nicht durch Blockierregeln blockiert sind. Tippen Sie auf das **Menü**-Symbol in der oberen rechten Ecke des Bildschirms und anschließend auf **Blockieren**, um eine der hier aufgelisteten Anwendungen zu blockieren. Daraufhin wird die Anwendung in die Liste **Blockierte Anwendungen** verschoben (in **Anwendungskontrolle** > **Blockieren**).

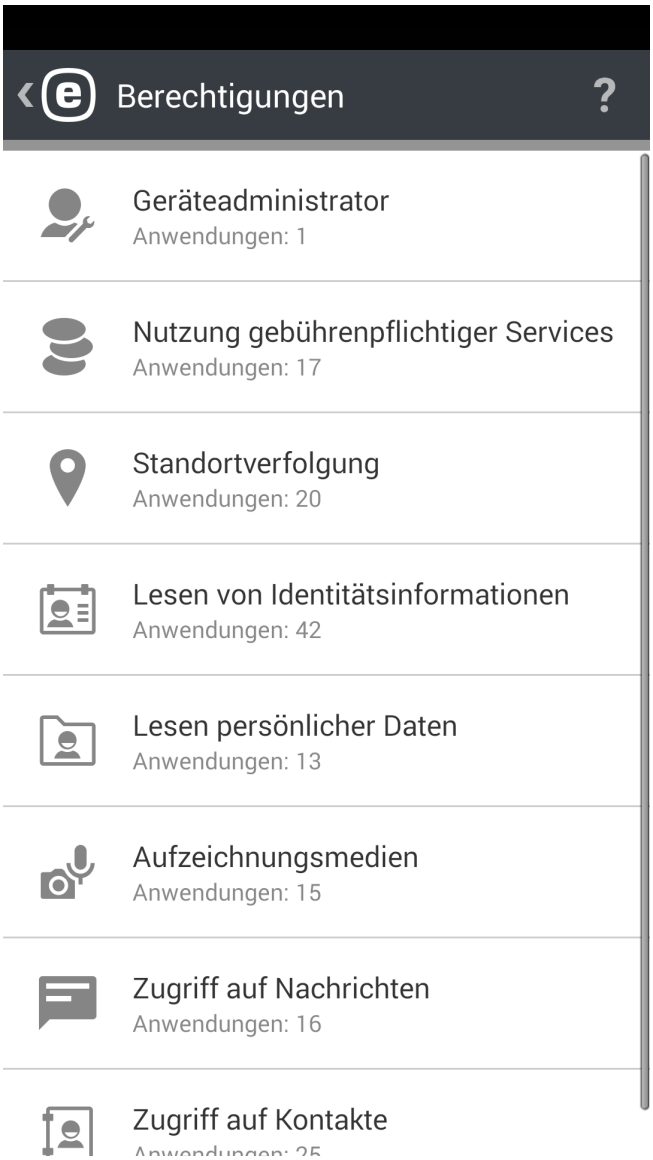


9.4 Berechtigungen

Mit dieser Funktion können Sie das Verhalten von Anwendungen verfolgen, die Zugriff auf persönliche Daten oder vertrauliche Unternehmensdaten haben. Administratoren können den Anwendungszugriff auf Grundlage vordefinierter Berechtigungskategorien überwachen.

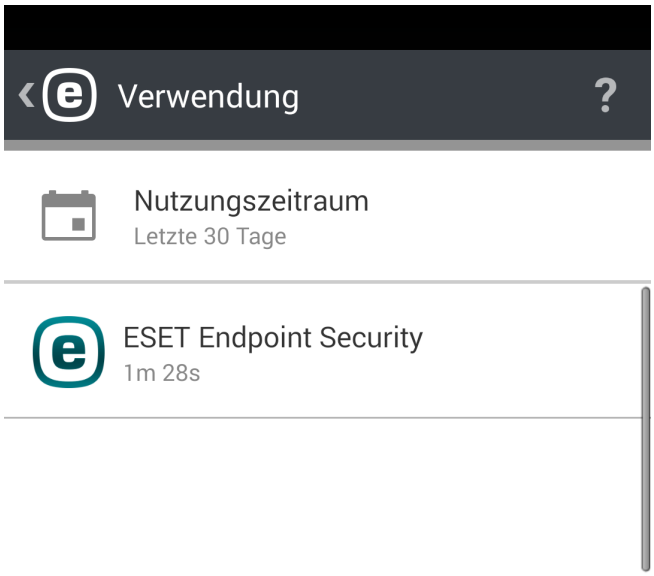
Manche Anwendungen auf Ihrem Gerät haben Zugriff auf Dienste, die Geld kosten, Ihren Standort nachverfolgen oder Ihre Identitätsdaten, Kontakte oder Textnachrichten auslesen. ESET Endpoint Security bietet eine Auditfunktion für diese Anwendungen.

In diesem Abschnitt wird eine Liste der Anwendungen nach Kategorien sortiert angezeigt. Tippen Sie eine Kategorie an, um deren Beschreibung anzuzeigen. Tippen Sie eine Anwendung an, um deren Berechtigungsdetails anzuzeigen.


Berechtigungen
Geräteadministrator
Anwendungen: 1
Nutzung gebührenpflichtiger Services
Anwendungen: 17
Standortverfolgung
Anwendungen: 20
Lesen von Identitätsinformationen
Anwendungen: 42
Lesen persönlicher Daten
Anwendungen: 13
Aufzeichnungsmedien
Anwendungen: 15
Zugriff auf Nachrichten
Anwendungen: 16
Zugriff auf Kontakte

9.5 Verwendung

In diesem Bereich können Administratoren die Dauer der Verwendung bestimmter Anwendungen durch Benutzer überwachen. Über die Option **Nutzungszeitraum** können Sie die Anwendungsliste nach Zeitraum filtern. Geben Sie an, ob Sie die Anwendungsverwendung der letzten 30 Tage, der letzten 7 Tage oder der letzten 24 Stunden anzeigen möchten.

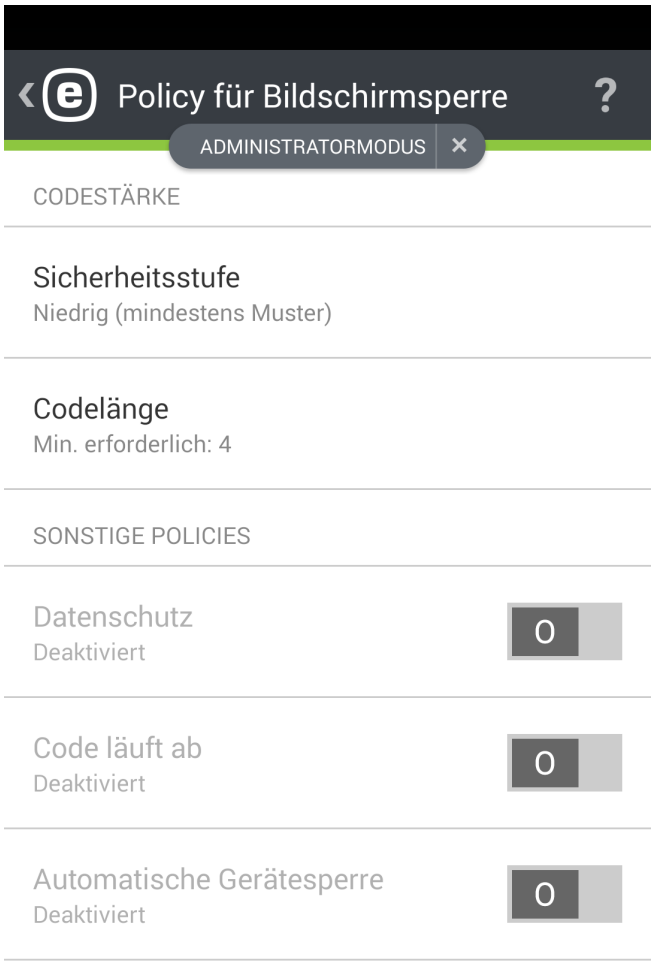


10. Gerätesicherheit

Unter **Gerätesicherheit** können Administratoren folgende Aufgaben ausführen:

- grundlegende Sicherheits-Policies auf Mobilgeräten anwenden und Policies für wichtige Geräteeinstellungen definieren
- die erforderliche Stärke der Bildschirmsperre festlegen
- die Verwendung integrierter Kameras einschränken

10.1 Policy für Bildschirmsperre



In diesem Bereich kann der Administrator folgende Aktionen ausführen:

- Mindestsicherheitsstufe (Muster, PIN, Passwort) für die Bildschirmsperre des Geräts und die Komplexität des Codes (beispielsweise Mindestcodelänge) festlegen
- maximale Anzahl nicht erfolgreicher Entsperrversuche festlegen (bevor das Gerät auf die Werkseinstellungen zurückgesetzt wird)
- Höchstalter für den Code der Bildschirmsperre festlegen
- Zeitgeber für die Bildschirmsperre definieren

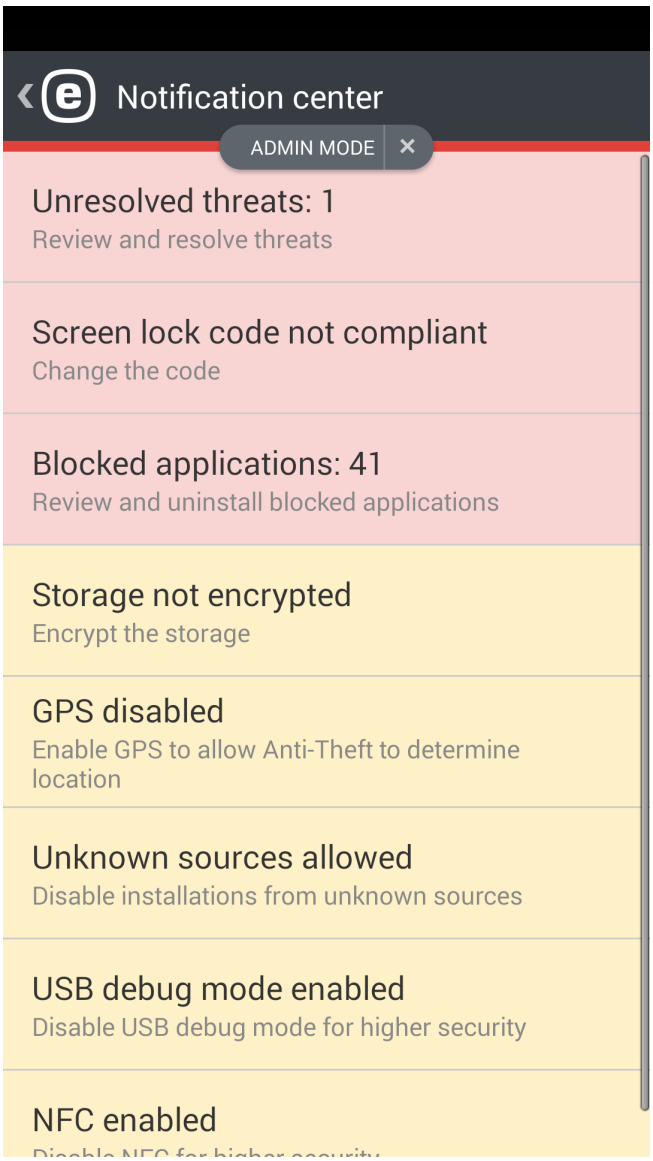
ESET Endpoint Security benachrichtigt automatisch den Benutzer und den Administrator, wenn die aktuellen Geräteeinstellungen die Sicherheitsrichtlinien des Unternehmens erfüllt. Wenn ein Gerät bestimmte Regeln verletzt, zeigt die Anwendung automatisch Vorschläge zum Beheben des Problems an.

10.2 Policy für Geräteeinstellungen

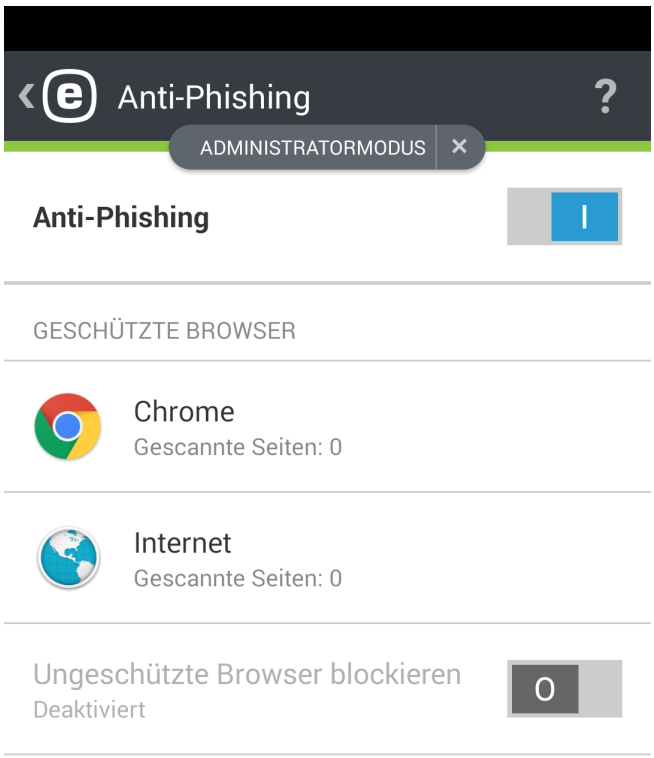
In der Gerätesicherheit ist auch die Option **Policy für Geräteeinstellungen** enthalten (früher Bestandteil des Sicherheits-Audits), über die der Systemadministrator vordefinierte Geräteeinstellungen überwachen kann, um zu ermitteln, ob sie dem empfohlenen Zustand entsprechen.

Die Geräteeinstellungen umfassen folgende Elemente:

- WLAN
- GPS-Satelliten
- Standortdienste
- Speicher
- Daten-Roaming
- Anruf-Roaming
- Unbekannte Quellen
- Debug-Modus
- NFC
- Speicherverschlüsselung
- Gerät mit Root-Installation



11. Phishing-Schutz



Der Begriff *Phishing* bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Daten zu erlangen, wie Kontonummern, Kreditkartennummern, PIN-Codes oder Benutzernamen und Passwörter.

Wir empfehlen, den **Phishing-Schutz** aktiviert zu lassen. Alle potenziellen Phishing-Angriffe von Websites oder Domänen, die in der ESET-Schadcodedatenbank enthalten sind, werden blockiert und es wird ein Warnhinweis angezeigt, der Sie über den Angriff informiert.

Der Phishing-Schutz kann in die gängigen für das Android-Betriebssystem verfügbaren Webbrowser integriert werden (zum Beispiel Chrome oder der standardmäßige Android-Webbrowser). Andere Browser werden als nicht geschützt aufgeführt. Sie können den Zugriff auf diese Browser durch Klicken auf den Schalter blockieren.

Um den Phishing-Schutz in vollem Umfang zu nutzen, empfehlen wir, alle nicht unterstützten Webbrowser zu blockieren, damit die Benutzer nur die unterstützten Browser verwenden.

HINWEIS: Beim Browsen im privaten Modus kann der Phishing-Schutz keinen Schutz bieten.

12. SMS- und Anruffilter

Der **SMS- und Anruffilter** blockiert eingehende SMS-/MMS-Nachrichten und eingehende oder ausgehende Anrufe je nach benutzerdefinierten Regeln.

Nicht angeforderte Nachrichten enthalten oft Werbungen von Mobildienstanbietern oder von unbekannten oder nicht identifizierten Benutzern. Beim „Blockieren“ einer Nachricht wird eine eingehende Nachricht automatisch in de Bereich **Verlauf** verschoben. Beim Blockieren einer eingehenden Nachricht oder eines eingehenden Anrufs wird keine Benachrichtigung angezeigt. Dies bietet den Vorteil, dass Sie nicht durch unerwünschte Informationen gestört werden, jedoch stets die Logs auf Nachrichten prüfen können, die fälschlicherweise blockiert wurden.

HINWEIS: Der SMS- und Anruffilter funktioniert nicht auf Tablets, die Anruf- und Nachrichtenfunktionen nicht unterstützen. Der SMS/MMS-Filter ist nicht für Geräte mit Android 4.4 (KitKat) verfügbar und wird auf Geräten, auf denen Google Hangouts als primäre SMS-Anwendung festgelegt ist, deaktiviert.

Um Anrufe und Nachrichten von der Telefonnummer des letzten eingehenden Anrufs zu blockieren, tippen Sie auf **Letzten Anrufer blockieren** oder auf **Letzten SMS-Absender blockieren**. Dadurch wird eine neue Regel erstellt.

12.1 Regeln

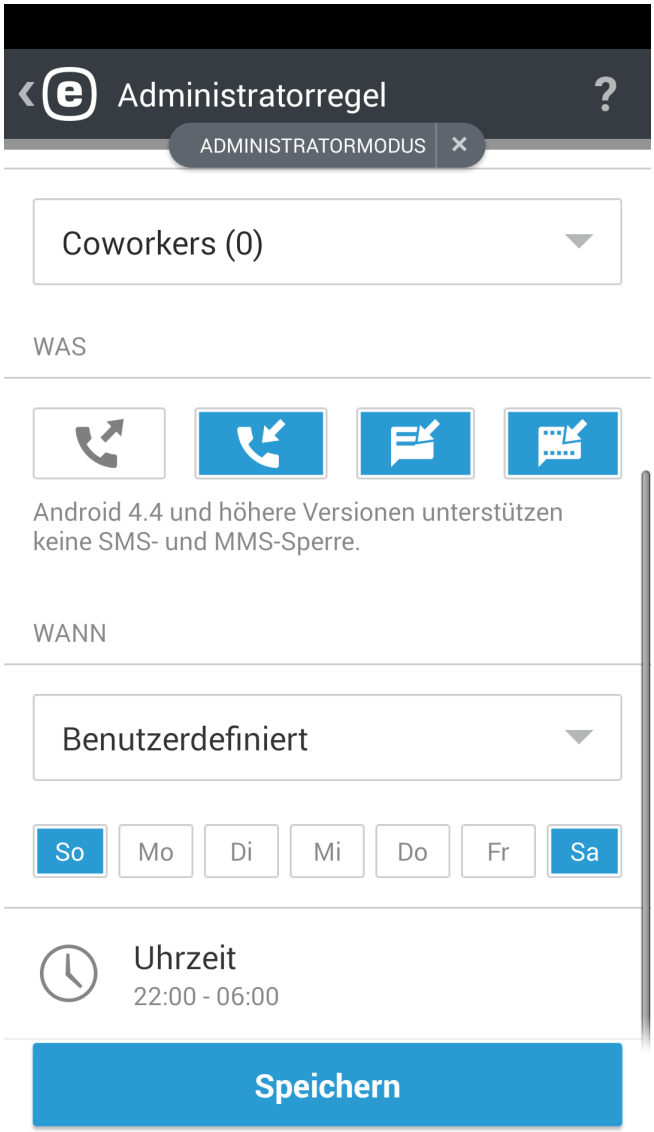
Benutzer können ohne Eingabe des Administratorpassworts Benutzerregeln erstellen. Administratorregeln können nur im Administratormodus erstellt werden. Alle Administratorregeln haben eine höhere Priorität als Benutzerregeln.

Weitere Informationen zum Erstellen einer neuen Regeln finden Sie in diesem Abschnitt.

Wenn Sie einen vorhandenen Regeleintrag aus der Liste **Regeln** entfernen möchten, tippen Sie auf den Eintrag und halten Sie ihn gedrückt. Tippen Sie dann auf das Symbol **Entfernen** .

12.1.1 Hinzufügen einer neuen Regel

Um eine neue Regel hinzuzufügen, tippen Sie auf das Symbol ➕, das sich oben rechts im Bildschirm **Regeln** befindet.



Wählen Sie aus, ob die Regel die Nachrichten und Anrufe zulassen oder blockieren soll.

Geben Sie eine Person oder eine Gruppe von Telefonnummern an. ESET Endpoint Security erkennt die Kontaktgruppen Ihrer Kontaktliste (zum Beispiel „Familie“, „Freunde“, „Kollegen“). **Alle unbekannten Nummern** umfasst alle Telefonnummern, die nicht in der Kontaktliste gespeichert sind. Mit dieser Option können Sie unerwünschte Telefonanrufe (zum Beispiel Kaltakquiseanrufe) blockieren oder verhindern, dass Mitarbeiter unbekannte Telefonnummern anrufen. Die Option **Alle bekannten Nummern** bezieht sich auf alle in der Kontaktliste gespeicherten Telefonnummern. Die Option **Unterdrückte Nummern** bezieht sich auf Telefonnummern, deren Übertragung absichtlich mit der Rufnummernunterdrückung (CLIR) ausgeschlossen wurde.

Geben Sie an, was blockiert oder zugelassen werden soll:

- ausgehende Anrufe
- eingehende Anrufe
- eingehende Textnachrichten (SMS)
- eingehende Multimedia-Nachrichten (MMS)

Um eine Regel nur vorübergehend anzuwenden, tippen Sie auf **Immer** > **Benutzerdefiniert** und wählen Sie die Wochentage und ein Zeitintervall für das Anwenden der Regel aus. Standardmäßig sind „Samstag“ und „Sonntag“ ausgewählt. Sie können diese Funktion beispielsweise einsetzen, um während einer Besprechung, auf Geschäftsreisen, in der Nacht oder am Wochenende nicht gestört zu werden.

HINWEIS: Zur Verwendung im Ausland müssen alle Telefonnummern in der Liste die internationale Vorwahl enthalten (zum Beispiel +49123456789).

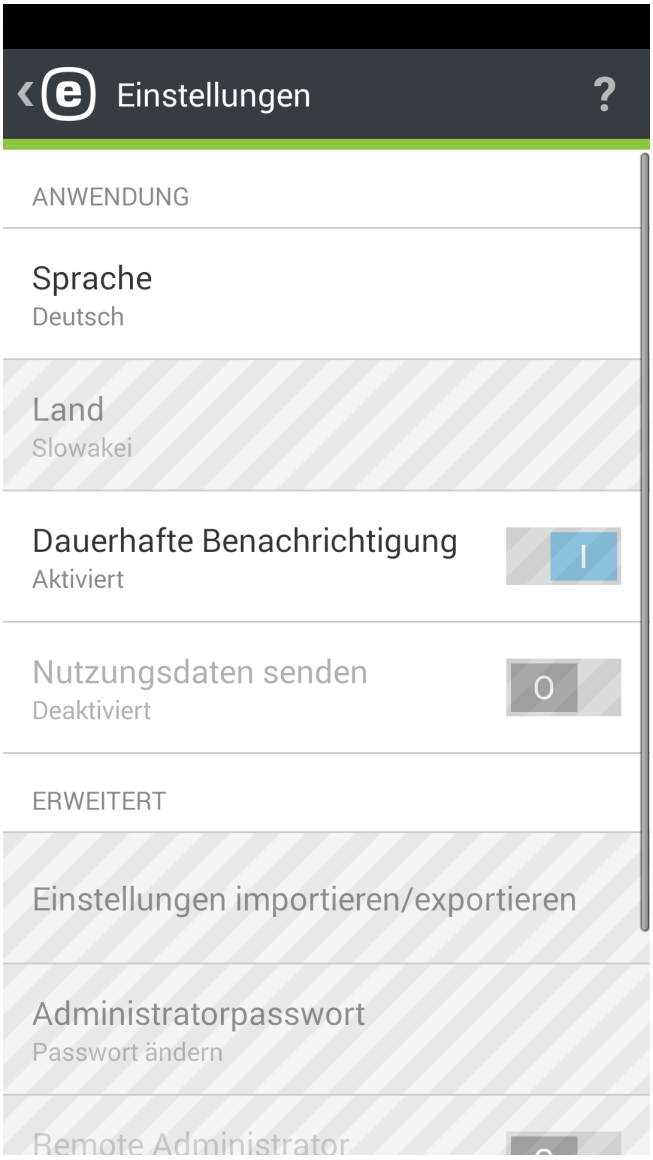
12.2 Verlauf

Im Bereich **Verlauf** werden die vom SMS- und Anruffilter blockierten und zugelassenen Anrufe und Nachrichten angezeigt. Jeder Log-Eintrag enthält den Namen des Ereignisses, die entsprechende Telefonnummer und Datum und Uhrzeit des Ereignisses. Logs für SMS- und MMS-Nachrichten enthalten außerdem den Nachrichtentext.

Wenn Sie eine Regel zu einer blockierten Telefonnummer oder zu einem blockierten Kontakt ändern möchten, wählen Sie den Eintrag durch Antippen in der Liste aus und tippen Sie auf das Symbol .

Um einen Eintrag aus der Liste zu entfernen, wählen Sie ihn aus und tippen Sie auf das Symbol . Um mehrere Einträge zu entfernen, berühren Sie einen der Einträge, halten Sie ihn gedrückt und wählen Sie die zu entfernenden Einträge aus. Tippen Sie dann auf das Symbol .

13. Einstellungen



Sprache
Standardmäßig wird ESET Endpoint Security in der Sprache installiert, die auf dem Gerät als Gebietsschema festgelegt ist (in den Sprach- und Tastatureinstellungen des Android-Betriebssystems). Um die Sprache der Benutzeroberfläche der Anwendung zu ändern, tippen Sie auf „Sprache“ und wählen Sie die gewünschte Sprache aus.

Land
Wählen Sie das Land aus, in dem Sie arbeiten oder leben.

Update
Um maximalen Schutz zu gewährleisten, sollten Sie stets die neueste Version von ESET Endpoint Security verwenden. Tippen Sie auf **Update**, um zu ermitteln, ob eine neuere Version zum Herunterladen von der ESET-Website bereitsteht. Diese Option ist nicht verfügbar, wenn Sie ESET Endpoint Security aus Google Play heruntergeladen haben. In diesem Fall wird das Produkt über Google Play aktualisiert.

Dauerhafte Benachrichtigung

ESET Endpoint Security zeigt das Benachrichtigungssymbol oben links im Bildschirm (Android-Statusleiste) an. Wenn Sie dieses Symbol nicht anzeigen möchten, deaktivieren Sie **Dauerhafte Benachrichtigung**.

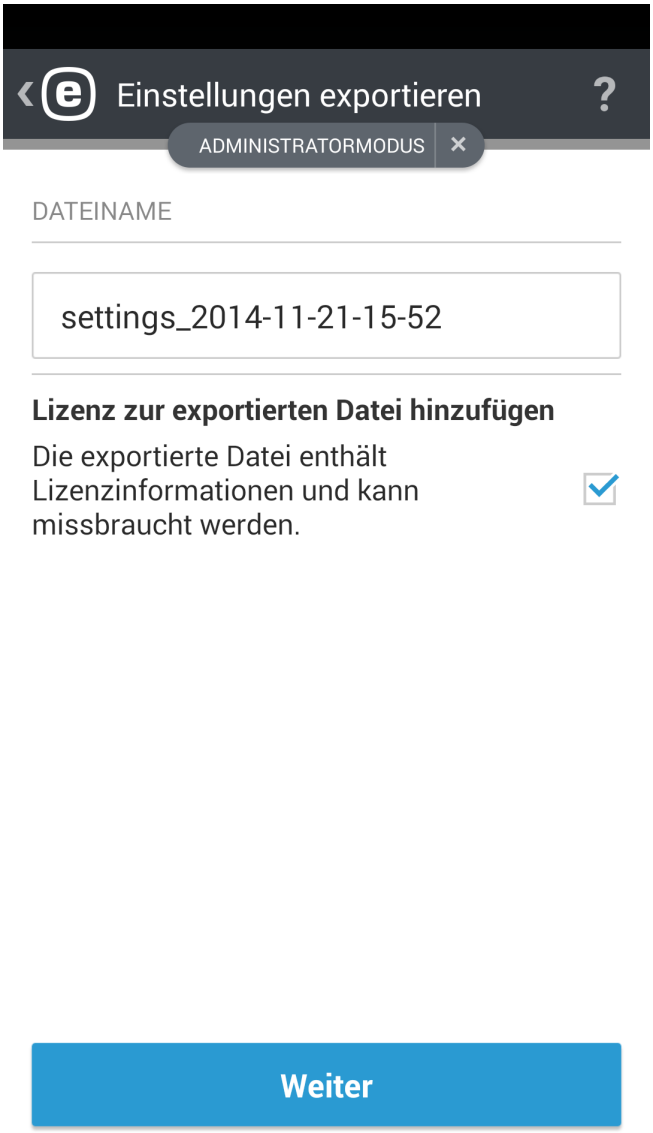
Nutzungsdaten senden
Mit dieser Option können Sie durch das Senden anonymer Daten über die Anwendungsnutzung zur Verbesserung der ESET-Produkte beitragen. Wenn Sie diese Option im Installations-Assistenten nicht ausgewählt haben, können Sie dies später im Bereich **Einstellungen** tun.

Administratorpasswort
Über diese Option können Sie ein neues Administratorpasswort festlegen oder das bestehende Passwort ändern. Weitere Informationen finden Sie im Abschnitt Administratorpasswort dieses Dokuments.

Deinstallieren
Wenn Sie den Deinstallationsassistenten ausführen, werden ESET Endpoint Security und die Quarantäneordner dauerhaft vom Gerät entfernt. Wenn der Deinstallationsschutz aktiviert wurde, werden Sie aufgefordert, das **Administratorpasswort** einzugeben.

13.1 Einstellungen importieren/exportieren

Um Einstellungen zwischen Mobilgeräten teilen zu können, wenn diese nicht mit ERA verwaltet werden, bietet ESET Endpoint Security 2 nun die Möglichkeit, Programmeinstellungen zu exportieren und importieren. Der Administrator kann die Geräteeinstellungen manuell in eine Datei exportieren und diese Datei (zum Beispiel per E-Mail) mit den Benutzern teilen. Die Datei kann auf einem beliebigen Gerät importiert werden, auf der die Clientanwendung ausgeführt wird. Wenn der Benutzer die Einstellungsdatei öffnet und akzeptiert, werden automatisch alle Einstellungen festgelegt und die Anwendung aktiviert (sofern die Lizenzinformationen enthalten waren). Alle Einstellungen sind mit dem Administratorpasswort geschützt.



13.1.1 Einstellungen exportieren

Um die aktuellen Einstellungen von ESET Endpoint Security zu exportieren, geben Sie einen Namen für die Einstellungsdatei an. Das aktuelle Datum und die Uhrzeit werden automatisch an den Dateinamen angehängt. Sie können auch die Lizenzinformationen (Lizenzschlüssel oder E-Mail-Adresse und Passwort des Sicherheitsadministratorkontos) in die exportierte Datei einfügen. Beachten Sie jedoch, dass diese Informationen nicht verschlüsselt werden und missbraucht werden können.

Wählen Sie im nächsten Schritt, wie die Datei übertragen werden soll:

- WLAN-Netzwerk
- Bluetooth
- E-Mail
- Gmail
- Dateibrowser (zum Beispiel ASTRO File Manager oder ES File Explorer)

13.1.2 Einstellungen importieren

Um Einstellungen aus einer Datei auf dem Gerät zu importieren, suchen Sie mit einem Dateibrowser wie ASTRO File Manager oder ES File Explorer die Einstellungsdatei und wählen Sie ESET Endpoint Security.

Sie können die Einstellungen auch importieren, indem Sie im Bereich **Verlauf** eine Datei auswählen.

13.1.3 Verlauf

Im Bereich **Verlauf** wird die Liste der importierten Einstellungsdateien angezeigt. Es stehen Funktionen zum Teilen, Importieren oder Entfernen dieser Dateien zur Verfügung.

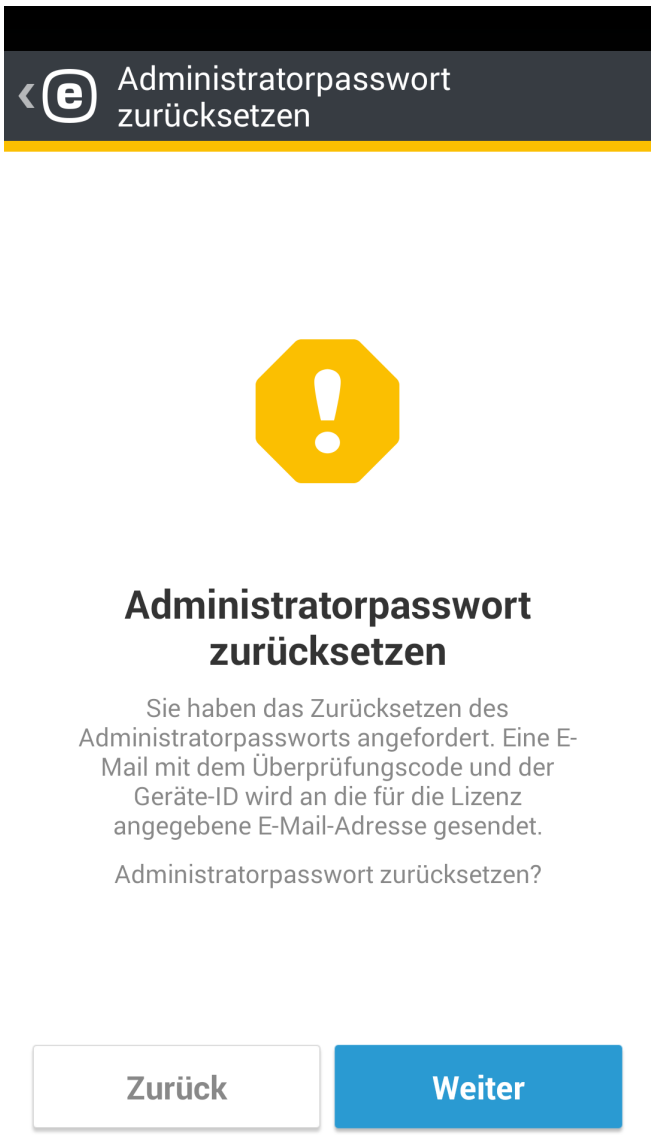
13.2 Administratorpasswort

Das **Administratorpasswort** wird für das Entsperren eines Geräts, das Senden von Anti-Theft-Befehlen, den Zugriff auf passwortgeschützte Funktionen und die Deinstallation von ESET Endpoint Security benötigt.

WICHTIG: Wählen Sie Ihr Passwort mit Bedacht. Verwenden Sie eine Kombination aus Groß- und Kleinbuchstaben und Ziffern, um ein sicheres Passwort zu erstellen, das schwer zu erraten ist.

So setzen Sie das Administratorpasswort auf einem Gerät mit gesperrtem Bildschirm zurück:

1. Tippen Sie auf **Passwort vergessen?** > > **Weiter** > **Überprüfungscode anfordern**. Falls das Gerät nicht mit dem Internet verbunden ist, tippen Sie stattdessen auf den Link **Passwort offline zurücksetzen** und kontaktieren Sie den ESET-Support.
2. Rufen Sie Ihre E-Mails ab - eine E-Mail mit dem Überprüfungscode und der Geräte-ID wird an die mit der ESET-Lizenz verknüpfte E-Mail-Adresse geschickt. Der Überprüfungscode ist nach dem Erhalt 1 Stunde lang gültig.
3. Geben Sie den Überprüfungscode und ein neues Passwort im Sperrbildschirm Ihres Geräts ein.


Administratorpasswort zurücksetzen
Administratorpasswort zurücksetzen
Sie haben das Zurücksetzen des Administratorpassworts angefordert. Eine E-Mail mit dem Überprüfungscode und der Geräte-ID wird an die für die Lizenz angegebene E-Mail-Adresse gesendet.
Administratorpasswort zurücksetzen?
Zurück
Weiter

13.3 Remote administrator

Mit ESET Remote Administrator (ERA) können Sie ESET Endpoint Security in einer Netzwerkumgebung von einem zentralen Standort aus verwalten.

ERA erhöht die Sicherheit und vereinfacht die Verwaltung aller ESET-Produkte, die auf Client-Arbeitsstationen und Mobilgeräten installiert sind. Geräte mit ESET Endpoint Security können über eine beliebige Art Internetverbindung wie WiFi, LAN, WLAN oder Mobilfunknetz (3G, 4G, HSDPA, GPRS) eine Verbindung zu ERA herstellen. Es muss sich lediglich um eine reguläre Internetverbindung ohne Proxy oder Firewall handeln und die beiden Endgeräte müssen richtig konfiguriert sein.

Wenn über ein Mobilfunknetz eine Verbindung zu ERA hergestellt wird, hängt der Erfolg der Verbindung auch vom Netzanbieter ab und es muss eine Internetverbindung ohne Funktionseinschränkung zur Verfügung stehen.

Um ein Gerät mit ERA zu verbinden, fügen Sie das Gerät zur Liste **Computer** in der ERA-Webkonsole hinzu, registrieren Sie das Gerät mit dem Task **Geräteregistrierung** und geben Sie die Mobile Device Connector (MDC)-Serveradresse ein:

- **Server-Host** - Geben Sie den vollständigen DNS-Namen oder die öffentliche IP-Adresse des Servers an, auf dem Mobile Device Connector (MDC) ausgeführt wird. Der Hostname kann nur verwendet werden, wenn Sie die Verbindung über ein internes WLAN-Netzwerk herstellen.
- **Server-Port** - Hier können Sie den Server-Port angeben, der für die Verbindung zu Mobile Device Connector verwendet wird.

HINWEIS: Weitere Informationen zur Verwaltung eines Netzwerks mit ESET Remote Administrator finden Sie in der ESET Remote Administrator-Onlinedokumentation.

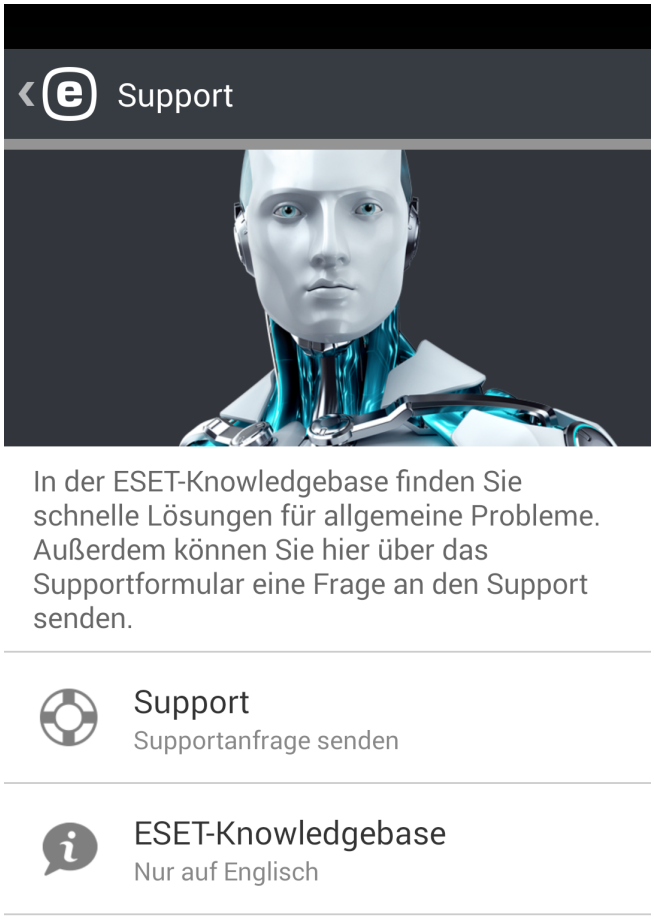
13.4 Geräte-ID

Anhand der Geräte-ID kann der Administrator Ihr Gerät leichter identifizieren, falls es verloren geht oder gestohlen wird.

14. Support

Die Experten vom ESET-Support stehen mit administrativer und technischer Unterstützung in Bezug auf ESET Endpoint Security und beliebige andere ESET-Produkte zur Verfügung.

Um direkt von Ihrem Gerät eine Supportanfrage zu senden, tippen Sie auf das Menüsymbol im Hauptbildschirm von ESET Endpoint Security (oder drücken Sie die Menütaste Ihres Geräts), tippen Sie auf **Support** > **Support** und füllen Sie alle Pflichtfelder aus.


Support
In der ESET-Knowledgebase finden Sie schnelle Lösungen für allgemeine Probleme. Außerdem können Sie hier über das Supportformular eine Frage an den Support senden.
Support
Supportanfrage senden
ESET-Knowledgebase
Nur auf Englisch

ESET Endpoint Security bietet eine erweiterte Protokollierungsfunktion zur einfacheren Diagnose möglicher technischer Probleme. Um ESET einen detaillierten Anwendungs-Log bereitzustellen, vergewissern Sie sich, dass **Anwendungs-Log senden** ausgewählt ist (Standard). Tippen Sie auf **Einreichen**, um Ihre Anfrage zu senden. Ein Experte vom ESET-Support wird sich unter der bereitgestellten E-Mail-Adresse mit Ihnen in Verbindung setzen.